5. Information Transfer

This chapter includes network communication standards and guidance for terrestrial wide area networks, wired and wireless local area networks, satellite communication networks, and internetworking protocols to link these together into a single integrated network. The relationship of this chapter with the ITSG is shown in Figure 5-1.

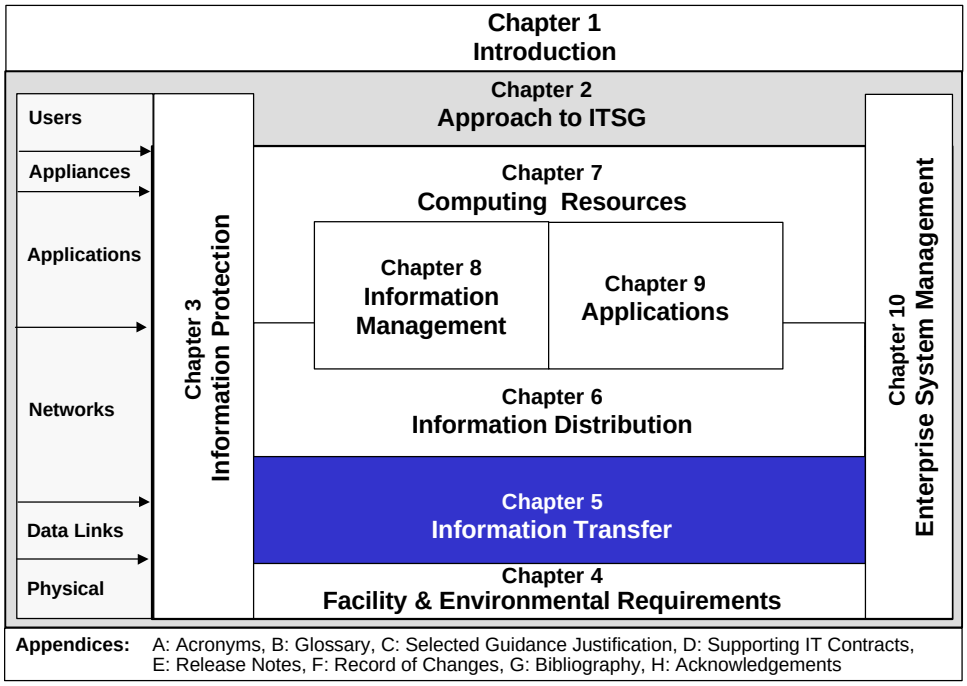

Figure 5-1. ITSG Document Map Highlighting Chapter 5, Information Transfer

5.1 Overview

Information Transfer encompasses the first four layers of the seven-layer International Standards Organization/Open Systems Interconnect (ISO/OSI) model: physical, data link, network and transport.[3] The proper selection of interface standards and protocols specified in this chapter will promote an interoperable and scaleable communications infrastructure for DON systems installed in each operational environment.[4]

The Navy and Marine Corps rely on voice, data, facsimile, video, and imagery at ever-increasing rates. The underlying infrastructure must be capable of supporting multimedia, offer a variety of quality-of-service options (to meet application bandwidth, delay and priority constraints), be scaleable in both size complexity and available bandwidth, and assure interoperability among other DOD and commercial information systems. The need for the user to interact with information and systems outside of their immediate surroundings is expanding – architectures must be global for

[3] In the Internet Protocol (IP) model, the Network and Transport layers are combined. Also, detailed descriptions of the physical cable plant are provided in Chapter 4.

[4] Operational environments are described in Section 2.6

our geographically dispersed and mobile commands but retain a local “look and feel” for operation.

Our information services can best be provided by a network-centric approach in which services and applications are built onto a robust, scaleable and survivable network infrastructure. This network infrastructure must provide an adaptable foundation for advances such as multicast (in which information is broadcast to either a small or wide range of users in an efficient manner), real-time systems (which have strict time-sensitive and priority requirements) and other fleet priority systems.

5.1.1 Operational Environment Considerations

The standards described here are for the most part generic to any DON environment. However, platform-specific issues are addressed where appropriate.

5.1.1.1 Shipboard

Shipboard networks, including those on submarines, require special consideration. Their operational requirements are extraordinarily demanding, their off-board bandwidth environment is constrained, and their facility and support requirements are unique. To satisfactorily address these challenges, commanders must base their implementations upon the specific guidance for networks aboard new construction and in-service ships in this document. These standards must address all mission critical systems requirements and include both hardware and software functions as part of the initial design and installation of a shipboard network. In addition, interfaces between real-time systems (e.g., fire control, weapons control systems) and non-real-time systems must strive to achieve interoperability.

5.1.1.2 Shore

Shore-based networks, especially those in R&D activities and system command centers, offer additional flexibility to take greater risks and to drive the design of deployable systems. These environments are needed to push the emerging technologies.

5.1.1.3 Ground

Current standards for deployed ground forces consist mainly of point-to-point Radio Frequency (RF) links. This will change as RF-based networks are developed. Until such time, however, networking guidance for ground forces is limited to that provided for small installations.

5.1.1.4 Aircraft

Aircraft represent a unique environment in that their internal networks are small. The information transfer standards, however, remain the same. As with deployed ground forces, future RF-based networks will be important in fulfilling the aircraft mission.

5.1.1.5 Spacecraft

The satellite environment is undergoing a major change. Historically, satellite links are described as “bent pipes” in which information is uplinked to a particular spacecraft and simply repeated or retransmitted downward. Systems currently being designed will behave as true networks in which the original data will be routed along a dynamically changing subset of satellites in the

"constellation" before being relayed back to earth. Access to these satellite networks will be through proprietary ground terminals via standard interfaces.

5.1.1.6 Individual Mobile Users

Transportable and mobile users are considered in this document although applicable standards are still evolving. A distinction is made between users who transport their nodes from one place to another without maintaining connectivity and those who *do* maintain connectivity. In either case, it is desirous to have users "take their environment with them".

5.1.2 Adopted Network Definition

The "area network" conventions adopted by the ITSG are shown in Figure 5-2.

Local Area Network (LAN). LAN*s* use the IEEE 802, ANSI, and ATM standards – the signals travel over optical fiber cable or copper wire and all network components are under the ownership and control of the network manager. They include wireless LANs that are generally designed to support untethered network-to-end-user connections. The control definition applies here. Extended LANs include base and campus networks

Wide Area Network (WAN). WANs are divided into two parts. The first is defined as trunk technology and switching (Telephony DS-n/T-n and Synchronous Optical Network (SONET) OC-n transport, and ATM and Frame Relay switching). For this part, the economic definition applies – the LAN provider will generally purchase these services rather than invest in wide-area equipment and cable. The second addresses what the telephone industry refers to as the "local loop", meaning the reach from the central office to the business or residence. In many cases, the customer may actually own such assets. (See Table 5-1 for an illustration of DS, T and OC link designations).

Metropolitan Area Network (MAN). MANs cover that ambiguous overlap where relatively wide area networks can take on the characteristics of a LAN or a WAN. MANs either use LAN technology extended over a "larger" regional area or use WAN technology – point-to-point links that connect a relatively high concentration of LANs together, within a "smaller" regional area.

Radio Communications to Dispersed Forces include Satellite Communications (SATCOM) and Line-of-Site (LOS) radio links to support trunk (router-to-router or switch-to-switch) connections to underway or deployed forces.

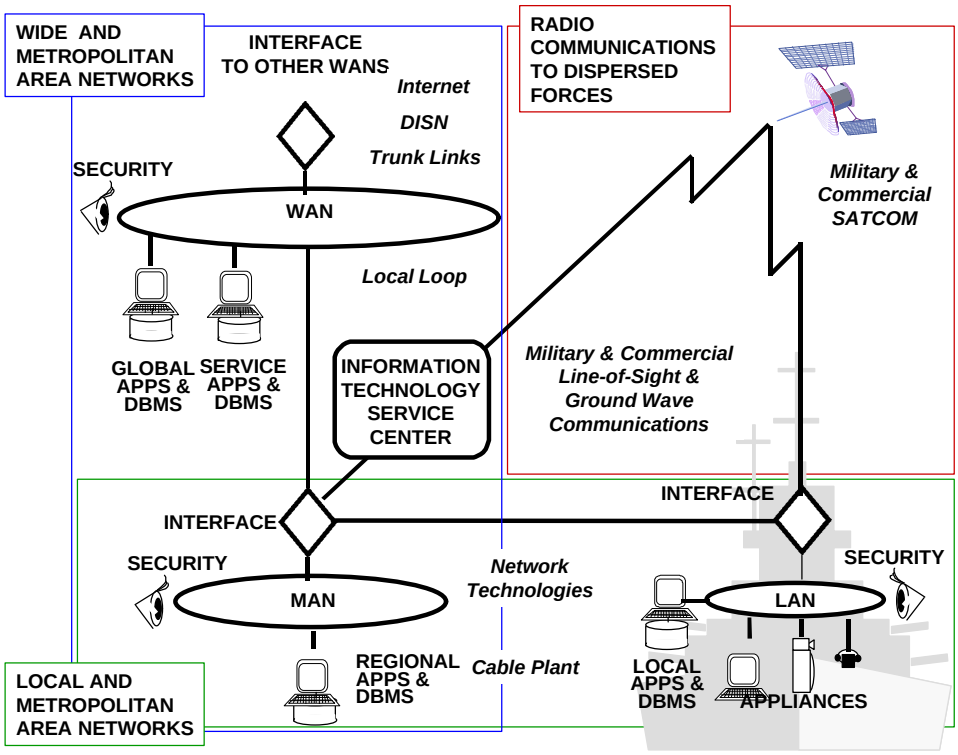

Figure 5-2. Adopted Architecture Model for LANs, MANs, WANs, and Radio Communication to Dispersed Forces

5.1.3 Performance Issues

To successfully design the information transfer infrastructure, system architects must ensure that operational requirements, including those of mission critical systems, are satisfied by the performance characteristics of the supporting IT systems. This is a challenging task, but new technologies are continually emerging that, if implemented in a standards compliant architecture, can dramatically improve the robustness of our infrastructure.

Throughput. Data throughput capacity is an important consideration in designing LANs and WANs. In the past, networks covering campuses and other small geographic distances could support significantly larger transfer rates than those that spanned large distances. Figure 5-3 illustrates the evolution of throughput over the last 20 years and Table 5-1 provides commonly used data rate designations. For example, in 1980 LANs employed 10 Mbps Ethernet while WANs employed 64 Kbps, DS-0 or 1.5 Mbps DS–1 for regional and long haul channels. This rate disparity began to diminish as LAN transfer rates increased to 100 Mbps through Fiber Distributed Data Interface (FDDI) and Fast Ethernet while WANs employed 45 Mbps, DS-3. Presently, transfer rates for local and long-haul networks have reached parity with OC-3/OC-12 SONET/ATM equipment and service. Future products are expected to continue this trend with 2.4 Gbps (OC-48) and 9.6 Gbps (OC-192) systems as well as Wave Division Multiplexing (WDM) technology (supporting 10's and 100's of independent 9.6 Gbps streams). As WAN transfer rates become comparable to those of the LANs, design emphasis must be placed on minimizing excessive processing of Protocol Data Units (PDUs) as they cross WAN-LAN boundaries (routers, firewalls, network filters, etc.).

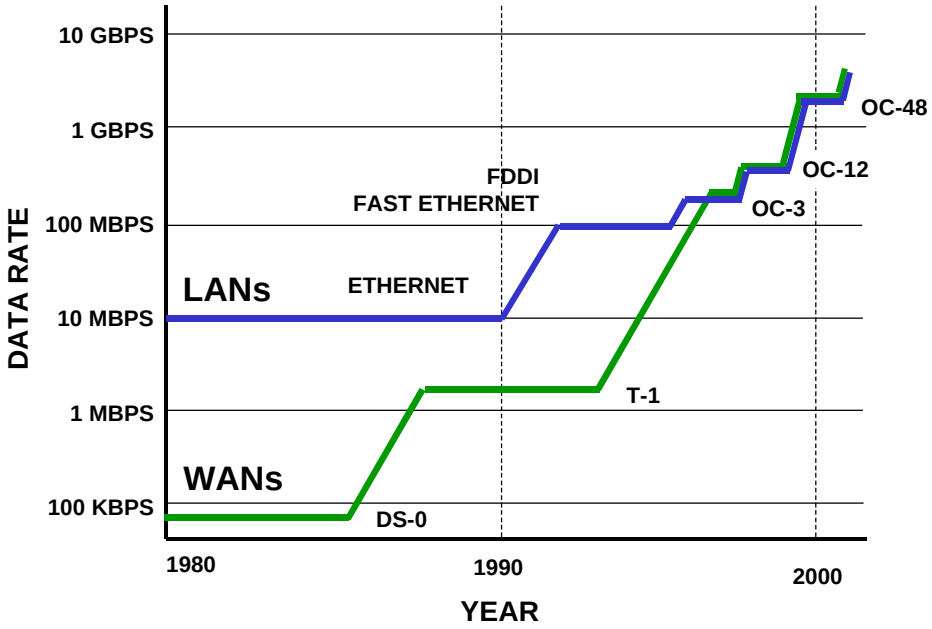

Figure 5-3. Evolution of LAN and WAN Data Throughput

Delay. Delay is another significant performance parameter that drives system design. Delay (with respect to networks) is composed of three significant components: propagation delay, processing delay and delay variation (or jitter). Electromagnetic propagation (including physical cables) has physical limitations that cannot be overcome. Propagation delays are simply a function of the geographic distance between points and cannot be reduced beyond these physical limits. By contrast, processing delays are nearly independent of distance and can range from insignificant, for electronic switching, to very significant, for the processing of data packets through CPUs, routers, firewalls, and network filters. Delay variation comes from many sources such as queues, physically different paths, RF media perturbation, etc. Delay variation, with respect to time, is a third design parameter.

Latency. The existing internet protocols provide best-effort service. In addition to the low-latency requirements of real-time systems, a number of applications require deterministic, or bounded-delay, service. Several next-generation initiatives, such as Asynchronous Transfer Mode (ATM), Reservation Protocol (RSVP), and next generation transport protocols, offer the promise of supporting bounded delay applications over a multi-segment internetwork. The recommended standards in this chapter will position the infrastructure to accommodate this capability as it matures.

Other performance measures may be used when the system has more rigid design constraints. For example, when designing for survivability in shipboard environments, the following apply:

Network Availability. The following network equipment performance requirements are necessary to support mission critical systems. The following operating modes are defined: normal, failure, and casualty. Normal mode is defined to be all network devices available and functioning. Failure mode is defined to be the malfunctioning of any two randomly selected network devices. Casualty mode is defined to be the non-availability of 25 percent of populated network port capacity. The network circuit availability of any single-homed user-to-user circuit shall be 0.999 or greater. The network availability of any redundant dual-

homed user-to-user circuit shall be 0.9999 or greater. The network system availability for mission-critical applications shall be 0.9999 or greater.

Data Rate Designation	Data Rate (rounded down)	Voice Quality Circuits 64 kbps	Full Motion Video Circuits 1.544 Mbps (note 1)	Remarks
DS0	64.0 kbps	1	-	Data Service - 0
T1	1.5 Mbps	24	1	Transmission Carrier -1
DS1	1.5 Mbps	24	1	Data Service - 1
DS1C	3.1 Mbps	48	2	Data Service - 1C
DS2	6.3 Mbps	96	4	Data Service - 2
Ethernet	10.0 Mbps	156	6	CSMA/CD (Note 2)
T3	44.7 Mbps	672	28	Transmission Carrier -3
DS3	44.7 Mbps	672	28	Data Service - 3
OC-1	51.8 Mbps	810	33	Optical Carrier - 1
Fast Ethernet	100.0 Mbps	1562	60	CSMA/CD (Note 2)
DS4N4	139.2 Mbps	2016	84	Data Service – 4N4
OC-3	155.5 Mbps	2430	101	Optical Carrier - 3
OC-9	466.0 Mbps	7218	301	Optical Carrier - 9
OC-12	622.0 Mbps	9720	405	Optical Carrier - 12
OC-18	933.0 Mbps	14,578	604	Optical Carrier - 18
Gigabit Ethernet	1.0 Gbps	15,625	647	CSMA/CD (Note 2)
OC-24	1.2 Gbps	18,750	777	Optical Carrier - 24
OC-36	1.9 Gbps	29,678	1230	Optical Carrier - 36
OC-48	2.5 Gbps	38,875	1619	Optical Carrier - 48
OC-96	4.9 Gbps	77,750	3239	Optical Carrier - 96
OC-192	9.6 Gbps	150,000	6217	Optical Carrier - 192

Table 5-1. Data Rate Designations

Note 1: Maximum value required for 30 frames/sec. Achievable at data rates as low as 384 kbps through compression.
Note 2: Carrier Sense Media Access / Collision Detect.

5.2 Physical and Data Link Layers

The physical and data link layers describe the lowest level of the ISO/OSI model (Figure 5-4). The physical layer is the actual channel on which data is transferred. The data link layer describes the protocol used directly on the physical layer medium. While the ISO/OSI describes these layers as separable, in practice they are tightly linked. In fact, there is usually a small number of recommended data link layer protocols associated with a particular physical layer specification and vice versa. Therefore, these bottom two layers will be discussed together.

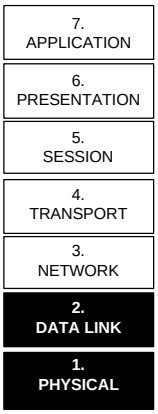

Figure 5-4. ISO/OSI model layers 1 and 2.

Physical channels include the fiber, copper and radio media upon which the data signals travel. Standards and. guidance associated with the cable plant are covered in Chapter 4. Radio media is discussed in Section 5.2.3.

5.2.1 Local and Metropolitan Area Network Physical and Data Link Layer Technologies

Best Practices

The preferred network architecture is a mesh topology of optical fiber running SONET on the physical layer and ATM on higher layers. Drop links to servers should be SONET/ATM linked to two physically separated switches. Appliances (end user devices) should be linked via fiber running (in order of preference) ATM, Switched Fast Ethernet, or Switched Ethernet. Category 5 UTP copper cable is permissible for the drop cable to non-mission critical appliances.

LAN configurations for the backbone, servers, mission critical appliances, and non-mission critical appliances should be consistent throughout the information system domain. Mixing of different protocols on like architectural components (e.g., all non-critical appliances) is not permitted except temporarily during the migration to an advanced protocol.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
ARCnet 100VG AnyLAN (802.12) Token Ring FDDI/UTP ANSI X3T12 SNA/APPN Novell IPX NetBEUI OpenAir 2.4 Wireless ETS 300 653 HIPERLAN Wireless	Switched Ethernet Switched Fast Ethernet FDDI SONET ATM UNI 3.1 for ATM PNNI Phase 1 for ATM	Switched Ethernet Switched Fast Ethernet SONET ATM UNI 3.1 for ATM UNI 4.0 for ATM PNNI Phase 1 for ATM	Switched Fast Ethernet SONET ATM UNI 3.1 for ATM PNNI Phase 1 for ATM UNI 4.0 for ATM	SONET ATM UNI 4.0 for ATM PNNI Phase 1 for ATM	Gigabit Ethernet IEEE Std 802.11-1997 (FHSS, 2 Mbps, 4-level GFSK) Wireless PNNI Phase 2 for ATM WDM
Activities, Platforms, Operational Environments		All			

Table 5-2. Physical and Data Link Recommended Implementations for LANs

There are a large number of technologies that fit in the physical and data link layer that can potentially be used in naval facilities. In the interest of balancing application flexibility with the logistics advantages of standardization, ITSG limits the selection to one, or a combination, of the following four network technologies: Ethernet, Fast Ethernet, FDDI and ATM.

Advantages and disadvantages of these lower layer networking technologies vary with the specific application, and are summarized in Figure 5-5.

Technology	Advantages	Disadvantages
Ethernet (10 Mbps)	Well understood Inexpensive Numerous vendors Strong commercial support Reliable multi-vendor interoperability Available in fiber version	Low throughput High latency Not scaleable as a backbone No fault tolerance No Quality of Service
Fast Ethernet (100 Mbps)	Moderate throughput Numerous vendors Strong commercial support Reliable multi-vendor interoperability Available in fiber version	Not scaleable as a backbone No fault tolerance No Quality of Service
FDDI (100 Mbps)	Moderate throughput Deterministic latency Fault tolerance Reliable multi-vendor interoperability Relatively easy upgrade from 10 Mbps Ethernet Inherently fiber	Expensive Not scaleable as a backbone without the use of FDDI switches Questionable future COTS support
ATM (155/622 Mbps)	High throughput Non-blocking Scaleable backbone Scaleable host performance Popular in WAN No need for routers to cross LAN/WAN boundary Available in fiber versions • Fault tolerance • Voice, Video and Data integration • Quality of Service	Limited multi-vendor interoperability Incomplete standards Limited multicast and broadcast support

Figure 5-5. Summary of Lower Layer Networking Technology

5.2.1.1 Ethernet

Ethernet is the most well understood networking technology in the commercial and tactical world. Ethernet is widely available in two different data rates: 10 Mbps and 100 Mbps.

Ten Mbps Ethernet is appropriate in situations that do not require extensive bandwidth and where cost is a driving issue. (Most network-ready devices and workstations have embedded 10 Mbps Ethernet.

Ten Mbps Ethernet is used for low-end workstations, but not for the backbone unless it is cost-driven; the implementation has a small number of users and is unlikely to expand.

5.2.1.2 Fast Ethernet

Fast Ethernet (100 Mbps) is the next generation of Ethernet technology and is undergoing wide deployment. Fast Ethernet is viable for the desktop and will soon be available pre-installed on PC motherboards. Note, however, that the fiber version (100BaseFX) is recommended for Navy shipboard use, not the unshielded twisted pair version (100BaseT).

Fast Ethernet may be used for workstation connections, but should not be used for the backbone unless it is cost-driven and the impact of its fixed, non-scaleable bandwidth and lack of inherent fault tolerance are understood, fully evaluated and meet the application requirements.

5.2.1.3 Gigabit Ethernet

Gigabit Ethernet, despite the name, is not based on traditional broadcast Ethernet. It is a point-to-point protocol that is expensive compared to other technologies, e.g. 10 Mbps to 100 Mbps Ethernet or ATM. It is a short-hauled router interconnect technology and not a WAN technology and has limited end station support. Gigabit Ethernet is an emerging technology, and its use is discouraged.

5.2.1.4 Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) is a 100 Mbps networking technology that uses counter-rotating token rings to provide moderate throughput with built-in fault-tolerance. Also, it has bounded deterministic delays, such as how long a station must wait before it can transmit, or how long it will take for a ring to reconfigure after segmentation.

FDDI technology is a technology for use where the advantages of rapid reconfiguration and bounded latency outweigh the uncertainty of future industry support. (The cost of FDDI has not reduced as other networking technologies. With its limited throughput and non-scaleability, vendors are pursuing other high-speed LAN/WAN technologies.) Where FDDI is used, it should be the standard fiber version; the copper version (sometimes called CDDI, FDDI/TP or FDDI/UTP) should not be used.

FDDI may be used for both critical workstation connections and for the backbones of a special purpose networks (e.g., for combat systems). However, FDDI should not be used as a shipwide backbone unless the impact of its fixed, non-scaleable bandwidth is understood and meets the application requirements.

5.2.1.4.1 Standalone Optical Bypass Switches

Optical bypass switches can be used to ensure that an FDDI ring does not segment in case of an end system losing power. However, it is preferable to design FDDI networks in such a way that standalone optical bypass switches are not needed. Optical bypass switches are subject to both signal loss and shock failures.

5.2.1.5 Synchronous Optical Network (SONET)

SONET is the ANSI broadband networking standard designed to meet the needs of high-bandwidth applications, increased data traffic, faster speeds, improved performance and a much greater degree of survivability. SONET uses a closed loop architecture that can recognize a cut or failure, rerouting traffic before serious performance degradation occurs, or in advance of a service interruption. The basic data rates available through SONET are referred to as “Optical Carrier” rates (Table 5-1) and are much higher than available on copper cable. In addition to setting new standard transmission rates, SONET standardizes frame formats and provisioning protocols for Operations, Administration and Maintenance (OAM).

5.2.1.6 Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is a networking technology that has several desirable properties such as scalability and quality of service. It is intended to support a large number of users, especially those who require, or will require, multimedia support. It has received wide support in the commercial sector, but associated standards are still maturing.

ATM is a technology that is suitable for the desktop, the backbone and the WAN. The preferred desktop ATM interface is 155 Mbps OC-3c (fiber). The 25Mbps Desktop ATM and the 155-UTP, both of which use unshielded twisted pair, are alternate choices, should cost be an issue. In shipboard environments, however, the use of copper is discouraged so 25Mbps and 155-UTP should be limited.

The 622 Mbps OC-12c interface may be used for inter-switch backbone trunks and high-speed host connections for devices such as servers. Given the use of Private Network to Network Interface (PNNI), the option of using a greater number of less-expensive OC-3c inter-switch trunks as an alternative to a smaller number of OC-12c trunks should be considered as a possible means of increasing the network’s reliability and survivability. (This only applies if the data rates of individual ATM virtual circuits are significantly less than OC-3c.)

ATM is a preferred backbone technology for new construction and major upgrades to all networks. Due to the current state of ATM interoperability, care should be taken when using ATM to assure that the same version of PNNI is used for all switches, and the same version of User to Network Interface (UNI) is used for all switches and workstations.

ATM is making great strides in WAN applications. In addition, many service providers are offering usage-based billing as an alternative to dedicated service. With this billing option, one could have on-demand access to high-speed transfer rates when the mission demanded. For example, one could contract for 155 Mbps peak service yet pay for 50 Mbps average throughput. When a need arose for higher throughput, one could start using more bandwidth through reconfiguration. (This would be much faster than requesting an upgraded circuit.)

5.2.1.7 Redundancy Techniques and Reconfiguration Time

All networks require some level of redundancy, particularly in the shipboard environment. Redundancy can be implemented under three broad techniques:

(a) **parallel transmission** over multiple paths

(b) **single active path** with one or more fail-over paths

(c) **load sharing** over multiple paths

For shore-based environments, option (c) load sharing, offers a cost-effective way to balance the need to provide redundancy against the need to provide bandwidth. Less critical applications could use the extra bandwidth until it was needed by the critical applications.

Redundancy techniques used for shipboard LANs should be limited to those techniques that are widely supported by industry. Special techniques, such as (a) parallel transmission, may be used in subsystems where the need for a particular form of redundancy, or rapid reconfiguration, can overcome the disadvantages of proprietary solutions. However, proprietary redundancy techniques should never be used in the ship-wide backbone.

Reconfiguration time, depending on the application, can be a critical design constraint. For example, a fire-control system would have a much tighter constraint than an administrative e-mail system. The use of proprietary systems to satisfy reconfiguration time criteria should be minimized.

Option (a), parallel transmission, offers the possibility of the most rapid reconfiguration because each receiving device can arbitrarily select one of multiple simultaneous channels, independent of other receiving devices.

Option (b), single active path, results in switchover or reconfiguration times that can range from 10s of milliseconds (in a small FDDI ring using Station Management (SMT) for reconfiguration) to 10s of seconds (for a large network using IEEE 802.1d Spanning Tree for reconfiguration).

Loadsharing with multiple paths typically achieves switchover in 5 to 15 seconds in a small to medium size ATM network using PNNI.

For a ship-wide ATM backbone, it is important to recognize that the current 5-15 second switchover time, combined with load-sharing over multiple paths, occurs only if the ATM switches are running full Phase 1 (or later) PNNI. Phase 0 PNNI (also known as Interim Interswitch Signaling Protocol or IISP) does not provide inherent redundant path reconfiguration. Multiple paths with IISP must be resolved using spanning tree protocol, with its associated 30 - 90 second reconfiguration time.

ATM switches should use Phase 1 (or later) PNNI. The redundancy architecture should exploit PNNI reconfiguration in lieu of spanning tree reconfiguration. For critical subnets where the PNNI reconfiguration times are excessive, FDDI with SMT reconfiguration is preferred, and parallel transmission over multiple paths is a less desirable option.

Note that, for Ethernet or Fast Ethernet networks, the only widely supported, non-proprietary redundancy mechanism is Spanning Tree.

Caution: Any time a dual-homed device is connected to a network running Spanning Tree, the network will reconfigure to resolve the loop created by the dual-homed attachment. For this reason, it is unwise to use dual-homed laptops or other dual-homed workstations that are moved frequently.

For either single active path or load sharing over multiple paths:

- All backbone switches should be interconnected via multiple trunklines to different switches to avoid any single point of failure;
- All edge devices should be dual-homed to two different backbone switches;
- All servers should be dual-homed to two different network connection points.

5.2.1.8 Network Interface Cards (NICs)

When choosing a lower layer network technology to bring the network to a desktop system, the applications on the desktop system may drive the technology selected. Real-time applications, such as voice and video, require different capabilities of the underlying media than word processors and database applications. For example, 10 Mbps Ethernet may meet the requirements for exchanging e-mail and word processing documents between desktop systems, whereas 155 Mbps ATM may be more suitable for desktop systems supporting a full motion, high definition, video application. Care should be taken, however, in buying "too low." As traditional low rate applications require more band width, and new applications (as web browsing) emerge, one should plan for future growth by acquiring the fastest host interface that one can afford.

5.2.1.8.1 Ethernet NICs

When procuring a system with Ethernet, a NIC that supports auto-sensing 10/100 Mbps is recommended. Also, a fiber optic NIC can be used to support a future upgrade to FDDI or ATM without the need for re-cabling. However, see Chapter 4, Section 4.3.2.2 regarding the permissive use of Category 5 cable under special circumstances.

5.2.1.8.2 FDDI NICs

A station can be either dual-attached station (DAS) or a singly attached station (SAS) to an FDDI ring. A DAS, while more expensive than a SAS, can be configured for higher survivability.

5.2.1.8.3 ATM NICs

There are two key issues to consider when ATM NICs are used in end systems – the User-Network Interface (UNI) and ATM adaptation protocol support.

5.2.1.8.4 UNI (User-to-Network Interface)

When using ATM NICs, the version of UNI that is supported is critical. The UNI specifies how ATM end systems communicate with other ATM end systems and ATM switches. There is currently one acceptable version of the UNI: version 3.1. The newer version (4.0) has been completed, and supporting COTS products will soon be available.

It is required that all end systems using ATM as the underlying media support UNI version 3.1 or higher.

5.2.1.8.5 ATM Adaptation Protocols

When using ATM NICs, the support for specific ATM adaptation protocols must be determined. Currently, there are four options available in COTS ATM NICs:

- Proprietary Adaptations of IP
- Classical IP Over ATM (RFC 1577),
- LAN Emulation (LANE)

- Multiple Protocol Over ATM (MPOA)
- Native ATM.

Note that while LANE and some proprietary adaptations of IP over ATM support broadcast and multicast, RFC 1577 does not.

Proprietary adaptations of IP, Classical IP and LANE are viewed as near-term solutions that will be replaced by Multi-protocol Over ATM (MPOA). (Most ATM vendors have announced their intention to support MPOA and a number have already started to make Beta versions available to selected customers. Since this is a fast-moving area, users should contact vendors directly regarding delivery schedules.) The idea behind these solutions is to emulate the properties of broadcast media (such as Ethernet and FDDI) on ATM, which is a non-broadcast medium. These solutions do not currently take advantage of the quality-of-service features that are inherent to ATM. There are problems with broadcast and multicast traffic. Each protocol employs a server to emulate broadcast and multicast capabilities. This emulation creates throughput, survivability, and scaleability limitations in the approach. The server is a potential bottleneck for multiple broadcast and multicast traffic streams, and is also a single point of failure.

While use of native ATM corrects some of these problems; it introduces others in interoperability. Most ATM NIC software drivers include an Application Programmers Interface (API) that enables applications to access ATM directly, bypassing the transport and network layer protocols. This enables these applications to use certain quality-of-service functions of ATM. Currently, each vendor of ATM NIC cards has a unique, non-interoperable API, and the use of native ATM may preclude the use of COTS software until such time that APIs are standardized. (As of this writing, Microsoft has announced plans for a standardize WINSOCK driver that supports ATM directly. Also, a number of ATM vendors have announced their intention to support X/Open’s XTI API for UNIX systems.)

Best Practices

ATM NIC cards, which support both RFC 1577 and LANE should be used to promote interoperability now. Since MPOA implementations are beginning to emerge, users are encouraged to start with MPOA if it is available from the selected vendor. If an application requires access to the native ATM services, the API that is part of the NIC can still be used. If the multicast and redundancy capabilities of vendor proprietary adaptations of IP are needed, then that protocol can be used as an interim solution pending the availability of MPOA.

5.2.1.9 Network Configuration

5.2.1.9.1 Switched Versus Shared Hubs

Under many conditions, switching hubs provide a considerable performance improvement over shared-media hubs. Switched hubs will reduce packet collisions and provide greater effective bandwidth than shared-media hubs. In FDDI networks, the use of switched hubs would result in long (Spanning Tree) reconfiguration times instead of short FDDI wrap times achieved with a concentrator tree architecture.

The management of all devices connected to a shared-media hub is straightforward. The management device can see all of the connected devices given the broadcast nature of the shared media. For switched devices, the management device cannot directly see all of the switched ports. The two common solutions to this problem are port mirroring, where the port monitored is mirrored to a second port to which the management workstation is connected, or implementation

of an RMON 2 agent (or AMON agent for ATM) on the switch which collects management information from all ports and responds to SNMP requests from the management workstation. The port mirroring technique is limited and can monitor only one port at a time. For this reason, implementation of RMON 2 or AMON agent is recommended.

5.2.1.9.2 Virtual LANs and Emulated LANs

Virtual LANs (VLANs) and Emulated LANs (ELANs) provide a means for achieving the broadcast domain isolation of routing while retaining the throughput advantages of layer 2 switching. A VLAN is effectively standard TCP/IP running on top of ATM instead of Ethernet. An ELAN is one of what could be many virtual ATM LANs running on the same physical media. In a VLAN and ELAN environment, a number of vendor frame-tagging methods are not interoperable, and some VLANs may not be definable between multiple switches that are interconnected via a backbone.

5.2.1.9.2.1 Virtual LANs (VLANs)

There are four distinct types of VLANs, not all of which are supported by all vendors:

- VLANs defined by port number on the switch(es)
- VLANs defined by the MAC address of the user devices
- VLANs defined by the IP subnet mask of the user devices
- VLANs created automatically by commonality of IP subnet mask

Currently there are Virtual LAN capabilities being provided by most vendors of LAN switching products. Such Virtual LAN capabilities are intended to prioritize packets and limit broadcast and multicast packet transfers (which can reduce the effectiveness of switching capabilities if sent to all interconnected systems). Future capabilities of VLANs may include network management and security services. IEEE 802 has three efforts on-going to support an interoperable standards based Virtual LAN capability:

- Standard for Local and Metropolitan Area Networks – Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering (IEEE 801.1p)
- Draft Standard for Virtual Bridged Local Area Networks (IEEE 802.1Q)
- Link-layer Standard for Interoperable LAN Security (SILS) standard (IEEE 802.10)

5.2.1.9.2.2 Emulated LANs (ELANs)

Similar to that provided by VLANs in a conventional LAN environment, emulated LANs (ELANs) provide the ATM environment with a mechanism for isolating traffic and minimizing the propagation of unwanted broadcast messages. In a mixed Ethernet-ATM environment, ELANs and VLANs can be logically associated. A router, or some routing function, is needed to move data between different ELANs or VLANs.

Shipboard networks should provide appropriate VLAN support to embarked forces that meets the need for isolation of ship’s force subnets.

5.2.1.10 Network Components

5.2.1.10.1 Backbone Switches

5.2.1.10.1.1 Ethernet and Fast Ethernet Switches

Network devices that provide switched-Ethernet service fall into the following categories:

- Ethernet to Ethernet,
- Ethernet to Fast Ethernet uplink(s),
- Ethernet to FDDI uplink(s),
- Ethernet to ATM uplink(s),
- Fast Ethernet to Fast Ethernet,
- Fast Ethernet to ATM uplink(s).

Ethernet and Fast Ethernet switches should provide SNMP management support, and should include support of RMON 2. They should support VLANs, including VLANs defined by IP mask address.

5.2.1.10.1.2 FDDI Switches

FDDI switches provide the advantages of bandwidth scaleability when used in a peer-to-peer environment, and rapid switching when setup for cut-through switching. FDDI switches should provide a proxy-ARP (Address Resolution Protocol) function to support the normal ARP process that occurs on a shared-media FDDI ring. Note that loops created by redundant inter-switch paths will be resolved via Spanning Tree protocol, which is a very slow reconfiguration process. Where reconfiguration time must be minimized, use tree-connected FDDI concentrators that reconfigure rapidly using FDDI's SMT wrap protocol.

All FDDI switches should be capable of being managed via RMON2 and SNMP management devices.

5.2.1.10.1.3 ATM Switches

ATM switches should be non-blocking and should provide separate queuing for different QoS classes:

- Constant Bit Rate (CBR)
- Variable Bit Rate – Real Time (VBR-RT)
- Variable Bit Rate – Non Real Time (VBR-NRT)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

They should support UNI 3.1 and Phase 1 (or later) PNNI.

All ATM switches have similar cell switching times; however, call setup times vary widely. The calls/second rate of the switches must meet expected requirements.

If LANE Services (LANE Emulation Client Server (LECS), LANE Emulation Server (LES) and Broadcast/Unknown Server (BUS)) are to run on the backbone switches, determine the maximum BUS packet transfer rate (which varies widely among different switch vendors) and verify that it meets the expected requirements. In this context, note that unicast transfers to users whose addresses are not yet cached make use of the BUS services in LANE, so that a low-throughput

BUS can be overloaded even if there is no multicast or broadcast traffic. (If the BUS throughput performance with LANE services running on the backbone switches is inadequate, consider running the services on edge devices or on dedicated LAN Emulation Servers.)

Backbone ATM switches should be procured with dual, hot-swappable power supplies with separate AC power lines, and all line cards should be hot swappable.

All ATM switches used aboard Navy ships should be capable of being managed via RMON 2, AMON and SNMP management devices.

5.2.1.10.2 Edge Devices

Edge devices are needed whenever workstations of one type (e.g., Ethernet) must connect to a backbone of another type (e.g., FDDI or ATM). When edge devices are used in shipboard environments, they should be dual-homed to two different backbone devices for reliability and survivability reasons.

5.2.1.10.3 Modular Versus Fixed-Configuration Hubs

As stated, all backbone switches will be modular. However, edge devices are available in either a modular or fixed configuration option. The fixed configuration, (which consists of a single board with a fixed set of I/O ports), is less expensive than a modular hub but offers no flexibility for changing the interface mix. Where a hub needs to support a variable mixture of Ethernet, Fast Ethernet, FDDI and ATM interfaces, use a modular hub. In installations where a large number of workstations of the same interface type are located, consider use of fixed-configuration hubs to save cost.

5.2.1.10.4 Routers

Routers can be obtained in several configurations:

- Dedicated standalone routers – should be used whenever high-performance routing is needed.
- Routing functionality implemented within a hub and sharing processing power with other hub functions – may be used whenever routing is incidental to the hub function and is not expected to be the throughput bottleneck
- Routing software in workstations – should be avoided because routing is a resource intensive task that is best handled by dedicated hardware that is centralized to simplify network management.

5.2.1.11 Wireless LANs

Wireless LANs are a new but rapidly growing technology. The commercial marketplace is evolving rapidly, and it is difficult to provide stable guidance. The following is provided as near-term guidance, and will be updated as the market matures:

- As breakthroughs in this technology will be market-driven use commercial standards; do not implement wireless LANs using Navy-proprietary solutions.
- Use wireless LANs aboard ship only where mobility is an overriding consideration. Wireless LANs will always provide lower performance at a higher cost than wired LANs. Consider wireless LANs as a backup or mobile extension to a shipboard wired LAN; not

as a substitute for the wired LAN. Wireless LANs offer a potential contingency system to coordinate damage control aboard ships when the cable plant has been damaged.

- Do not use wireless LANs to transfer secure information. Wireless LANs do not provide the degree of security that can be obtained with fiber optic LANs. Information sent over wireless LANs can be intercepted by off-board listeners. Where security features must be added to wireless LANs, do so in a manner that does not result in a proprietary solution. (Encryption in the workstation with standard wireless LAN NICs is preferable to encryption embedded within the wireless LAN protocol.)

5.2.1.11.1 Wireless LAN Standards

The most widely used wireless LAN protocol in the past is the Wireless LAN Interoperability Forum OpenAir 2.4 Specification. The IEEE STD 802.11-1997 Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specification was approved on June 27, 1997. Although it is too early to predict how soon 802.11 wireless LANs will supplant OpenAir wireless LANs in popularity, the near-term guidance of this document is to favor the 802.11 standard over the proprietary OpenAir standard.

However, in spite of the approved IEEE standard, there is no guarantee that wireless LAN components from different vendors will interoperate. The 802.11 standard provides many options:

- Frequency Hopping Spread Spectrum Radio in the 2400-2483.5 MHz band:
  - 1 Mbps operation using 2-level Gaussian Frequency Shift Keying (GFSK)
  - Optional 2 Mbps operation using 4-level GFSK
- Direct Sequence Spread Spectrum Radio in the 2400-2483.5 MHz band:
  - 1 Mbps operation using Differential Binary Phase Shift Keying (DBPSK)
  - 2 Mbps operation using Differential Quadrature Phase Shift Keying (DQPSK)
- Infrared:
  - 1 Mbps using 16-position Pulse Position Modulation (16-PPM)
  - Optional 2 Mbps using 4-position Pulse Position Modulation (4-PPM)

The near-tern guidance for the use of Wireless LANs aboard naval ships is to use the IEEE 802.11 Frequency Hopping Spread Spectrum (FHSS) option at 2 Mbps data rate using 4-level GFSK.

While near-term guidance is to use the IEEE 802.11 FHSS standard, it is not the only non-proprietary wireless LAN standard. In Europe, the Escuela Tecnica Superior de Ingenieros (ETSI) HIPERLAN standard ETS 300 652 is being put forward as a potential worldwide standard. HIPERLAN has the advantage of supporting data rates up to 10 Mbps, but requires a wider bandwidth in a new frequency range around 5 GHz. Until recently, this band was illegal for use in the United States; however, on January 9, 1997 the FCC allocated 300 MHz of spectrum in the same band as HIPERLAN uses, thereby opening the possibility of 10 Mbps HIPERLAN wireless LANs in the near future. The use of HIPERLAN should be postponed pending its standardization within the U.S.

There is also work underway within the ATM Forum to develop a Wireless ATM standard; however, widespread use of wireless ATM should be postponed pending approval of the associated standards.

5.2.2 Wide and Metropolitan Area Network Physical and Data Link Layer Technologies

Best Practices

WAN services should be obtained through the Defense Information Systems Network (DISN). Internet services should be provided through Information Technology Service Centers (ITSCs) where required security measures can be provided. Wide area native ATM services should be preferably obtained from DISA. Where DISA service is not available or does not meet the price performance requirements, commercial ATM services can be used. ISDN is recommended for quick implementation of VTC services.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Commercial Internet Service Providers OpenAir 2.4 Wireless	DISN for IP Service DISA ATM Service (DAS) or Commercial ATM Service ISDN	DISN for IP Service DISA ATM Service (DAS) or Commercial ATM Service ISDN	DISN for IP Service DISA ATM Service (DAS) or Commercial ATM Service ISDN	DISN for IP Service DISA ATM Service (DAS)	IEEE STD 802.11-1997 Wireless xDSL
Activities, Platforms, Operational Environments		Shore			

Table 5-3. Physical and Data Link Recommended Implementations for WANs

5.2.2.1 Local Loop

The local loop is traditionally defined to be under the control of a local telephone company. This is the service provided between the Local Exchange Carrier (LEC) and the customer. (The term “local loop” originated from the fact that a standard two-wire Plain Old Telephone System (POTS) line is really a loop from the Central Office to the off-hook telephone and back to the Central Office.)

While such services are usually provided by the LEC, users on large installations who own their own “local loops” can use this technology as well. While this technology is not the preferred choice to extend one’s network, certain applications may benefit from these techniques. To repeat an earlier example, a remote guard shack 2 miles from the nearest network connection may need a multi-Mbps circuit for a camera and/or monitor. The cost to run fiber may be too prohibitive whereas an existing POTS line with the proper equipment may be adequate.

5.2.2.2 Digital Subscriber Line

Several closely related products known as xDSL (ADSL, RADSL, HDSL, SDSL, etc.) are designed to provide Mbps types of point-to-point communications over 1-3 mile copper segments (indeed, many telephone company DS-1 connections are really HDSL underneath but the handoff to the customer is DS-1). They use the higher frequencies that are normally filtered out in the telephone system by the 3kHz bandpass filters (commonly known as voice coils) for which telephone modems are forced to compensate. DSL products are useful for router-router, router-end system or end system-switch situations where it is important to salvage existing copper pairs and the copper run does not exceed the supported distances. This makes the technology attractive to sprawling bases or garrisons where the command owns the copper plant (and can remove the voice coils that prevent DSL technology from working). Because of the plethora of technologies, both ends of a DSL link should be purchased from the same, or guaranteed interoperable pair of, vendors. DSL technology should not be used in new installations where fiber optic cable plants should be installed.

5.2.2.3 ISDN

Integrated Services Digital Network (ISDN) is available in DON from either commercial off base providers or from a government owned or leased on-base switch network. ISDN is used for switched voice, data and video applications. The most prevalent application is for Video Teleconferencing where dedicated transmission is not cost effective. The majority of Navy (and DOD) shore VTC systems use ISDN as the transport media. ISDN is widely available in the continental US, Japan and Europe and is generally ordered in one of two transmission service types:

1. ISDN Primary Rate Interface (also known as PRI 23B+D service - 23 Bearer 64Kbps channels.

2. 1 Delta 64Kbps signal channel delivered from the telephone company on 4-wires) or ISDN Basic Rate Service (also known as BRI 2B+D – 2 Bearer 64Kbps channels and 1 64Kbps Delta channel delivered from the telephone company on 2-wires).

Especially well suited for geographically separated VTC users, ISDN delivers a cost effective usage based transmission service that allows for instant H.320 video calls on demand anywhere and anytime.

The following policy, guidelines and key factors for success should be followed if implementation of ISDN is required.

Best Practices

ATM is preferred as a WAN/MAN protocol over ISDN. However, if ATM is unavailable and ISDN is required to support VTC and low speed data connectivity, procure ISDN capable of Bearer Capability – CSD (Circuit Switched Data) 64Kbps Unrestricted Digital Information (UDI) also called “clear channel”.

- IMUX Capability – For data calls at rates above 128Kbps (i.e. 224, 256, 336 or 384Kbps) Bandwidth On Demand Interoperability Group (BONDING) Mode 1 multiplexing should be employed (see FIPS Pub 178). Note: When calls are originating and terminating on PRI service H0 (i.e. H0 384Kbps switched calls) preferred due to the guaranteed single

end to end clock source. End to end Local Exchange Carrier (LEC) - International Exchange Carrier (IXC) and IXC-LEC delivery capability is a problem with implementing this service – not all Regional Bell Operating Companies (RBOC) LEC and IXC companies are provisioned to handle this service due to present trunking and switch configuration schemes.

- National ISDN 1 - Customer Premise Equipment (CPE) must be NI1 compliant.

Guidelines

In planning any ISDN network several key items need to be taken into consideration:

- Who do you plan to communicate (VTC) with and what type of transmission service do they possess? If possible, order ISDN service with the same Inter-exchange Carrier (IXC) (AT&T or FTS-2000 etc.).
- What data rate is your VTC equipment capable of (128, 384 or 768Kbps)? Order ISDN service to match the highest data rate of your equipment or at least those of your distant end (i.e. single BRI for 128Kbps for desktop VTC as a minimum and Tri-BRI 384Kbps service (or PRI) for cart and room systems).
- What is the Concept of Operations for your VTC Network? If you plan to call OCONUS sites you will need to be PIC commercial ISDN IXC as your primary carrier, or if the majority of your distant end sites are FTS-2000 (FTS-2000 = 10387) you will want to order VON (Virtual Off Net) service from a commercial Carrier (i.e. AT&T Accunet =10288, MCI = 10222, Sprint = 10333). Note: Effective June 98 the FCC will be introducing the 7 digit PIC code (i.e. the new long distance carrier code for AT&T will be 1010288) IAW FCC rule 3DEC97 DA972528.TXT. Take note of this change and be prepared to modify ISDN access switch parameters (i.e. dial string - outgoing qualifiers) as required.
- How Many and What Type ISDN Drops Are Required? Should your plans require multiple (4 or more) dedicated BRI drops for locally distributed desktop VTC units, you may consider ordering a single PRI from the LEC and terminating it into an Inverse Multiplexer (i.e. Teleos Model 20 or Model 60) to distribute your own BRI S/T interface directly to the desktop. This local distribution method requires the use of Category 5 UTP wire from the IMUX to the desktop video terminals.
- For medium to large campus type ISDN distributed networks in which PRI and or multiple BRI's are employed, it is recommended that the Inverse Muliplexer (i.e. Teleos Model 60 or 200 Access Switch) be equipped with Q.921 and Q.931 protocol monitoring capability. The equipment should be capable of monitoring the status of Layer 1 physical (I.430), Layer 2 Link (Q.921) and Layer 3 Network (Q.931) protocols. This recommendation is made in order to aid the expediting of fault isolation (layer 2 and 3 debug) efforts.

Key Factors For Success

- ISDN Directory Numbers (DN's) – Ensure accuracy
- ISDN Service Profile Identifiers (SPIDs) – Ensure accuracy
- ISDN Switch Type (i.e. AT&T 5ESS, DMS-100 or Erricson) – Know the type switch you are connecting to and program your CPE (i.e., Terminal adapter or Inverse multiplexer) accordingly.
- ISDN Switch Software (i.e. NI-1 or Custom) – Again, know the type switch you are connecting to and program your CPE (i.e. Terminal adapter or Inverse multiplexer) accordingly.

- ISDN Capability Package – BRI's orders should specify V/C (V - voice and C – circuit switched data) for each B channel and P (Basic D Channel Packet) for the Delta Channel.
- ISDN NT1 (Network Termination 1 Device) Distance Consideration: The LEC (Local Exchange Carrier) will generally deliver a BRI U loop up to 18K' from the servicing Central Office (C/O) – when extending your U loop (in house) pay close attention to the length of your run to ensure it does not exceed 18K' in overall length. If in doubt contact your Telco to obtain BRI U length from the C/O to the LEC demarcation point on the premises.

5.2.2.4 Trunking

WAN connections originally consisted of 56 (or 64) Kbps circuits. These were increased to 1.5 Mbps DS-1 service (formerly called T-1) and 45 Mbps DS-3 service (formerly called T-3). Today's dedicated circuits can reach 155 Mbps (OC-3). The costs for these high-speed circuits is dramatically high (in some cases $500,000.00 per year for a single circuit connecting two sites). A number of methods can be used to cut this cost. First, DISA is standing up a high-speed CONUS network as part of the DISN (Defense Information Systems Network). Second, one can procure ATM services from DISA or a commercial carrier specifying both peak and sustained data rates. Usage above this rate is metered. Use of the Secret Internet Protocol Routing Network (SIPRNET) and the Non-classified Internet Protocol Routing Network (NIPRNET) is mandated for joint interoperability. The regional ITSCs will provide connectivity to the public Internet.

5.2.3 Radio Communications to Dispersed Forces

Best Practices

To participate in multi-media driven collaborative planning, and decision support operations, underway ships and deployed MEUs need a minimum standard data rate of 128 kbps during operations. This data rate is not yet economically achievable. Continued research, development, and acquisition should be sustained to attain this data rate. It is preferred that multiple independent communications paths be used for maximum fault tolerance. All media and all information classifications should be aggregated using appropriate technologies for multiplexing and encryption. Transitions between satellite footprints, between Line-of-Sight and SATCOM, from afloat to ashore, and from embarked to disembarked should be seamless.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
INMARSAT A, M	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B, C UHF LOS	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B, C UHF LOS	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B UHF LOS	UHF SATCOM SHF SATCOM EHF SATCOM GBS ATS INMARSAT B UHF LOS	Globalstar Iridium Orbcom Teledesic
Activities, Platforms, Operational Environments		Ship, Ground, ITSC			

Table 5-4. Physical and Data Link Recommended Implementations for Radio Communications to Dispersed Forces

The Naval Service is dependent upon exterior RF communication to maintain connectivity between its ashore, afloat and airborne command sites. RF links are also required to maintain coordination between the command sites and afloat tactical units. Standards exist for most military RF communications channels. Commercial RF communication channels often possess proprietary over-the-air interface standards, which prevent communication between equipment from different vendors. The Navy is developing internal standards for the transfers of high-speed data over radio WANs. Issues being addressed include data flow control, the termination of data delivery time, and prioritizing of data for delivery. Two such developments are the Afloat Telecommunications System (ATS) and Automated Digital Network System (ADNS). ADNS passes Internet Protocol (IP) datagrams, including multicast and router-to-router protocols.

Figure 5-6 is provided to illustrate the relationships between the various RF communication bands.

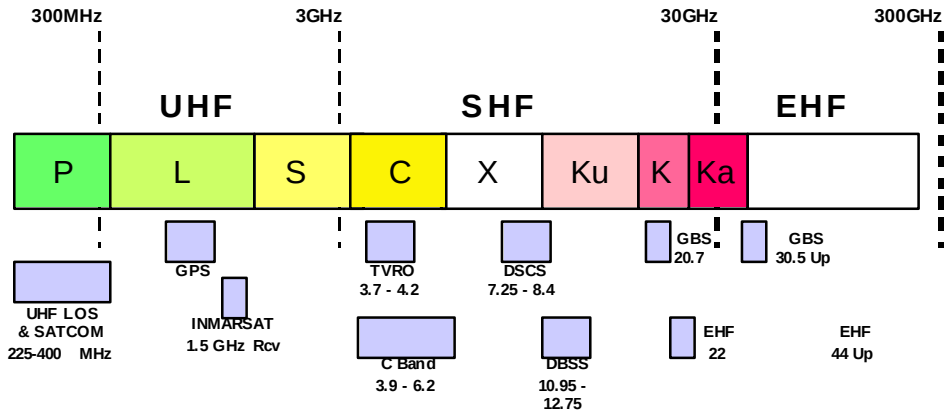

Figure 5-6. RF Bands Used in SATCOM

5.2.3.1 Military Satellite Communication (MILSATCOM)

MILSATCOM systems include those systems owned or leased and operated by the DoD. The basic elements of satellite communication consist of a space segment, control segment, and a terminal segment (air, ship, ground, etc.). An implementation of a typical satellite link will require the use of satellite terminals, user communication extension, and the use of military or commercial satellite resources.

The Navy UHF SATCOM System provides communication links, via satellites, between designated mobile units and shore sites. These links supply worldwide coverage between the latitudes of 70 degrees north and 70 degrees south. Multiple satellite constellations are currently in use: Fleet Satellite Communications System (FLTSATCOM), Leased Satellite (LEASAT), and the current series UHF Follow-On (UFO). The SATCOM system includes satellites, RF terminals, subscriber subsystems, personnel, training, documentation, and logistic support. The Navy SHF SATCOM system provides a high-capacity and jam resistant, full-duplex communication capability for high-value Naval combatants, special purpose ships, and selected shore sites. Defense Satellite Communication System Phase II (DSCS II) satellites and a second constellation of DSCS III satellites are currently being used for Navy SHF satellite communication. The Milstar satellite communication system is designed to meet the projected minimum essential wartime requirement associated with military communication. The system is survivable and jam resistant with Low-Probability-of-Intercept (LPI) and relay functions to meet strategic, tactical, and other associated communication needs. Block I satellites have growth capability via the Block II upgrade.

5.2.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards

Data and voice services are provided to the Navy via multiple services, 5 kHz, 25 kHz and 500 kHz transponder channels. One of the 25 kHz channels is used for broadcast purposes only. The remaining channels provide simplex communication within the technical limitations of the channel bandwidth. Navy UHF satellite communication is used to carry tactical communication traffic to and from the fleet. Approved crypto is required to secure all RF links and measures are taken to prevent hostile analysis.

5.2.3.1.1.1 5kHz and 25 kHz Service

For 5 kHz or 25 kHz single channel access service supporting the transmission of either voice or data, the following standard is mandated:

- MIL-STD-188-181A, Interoperability Standard for Single Access 5 kHz and 25 kHz UHF Satellite Communications Channels, 31 March 1997.

5.2.3.1.1.2 5kHz Demand Assigned Multiple Access (DAMA) Service

For 5 kHz DAMA service, supporting the transmission of data at 75-2400 bps and digitized voice at 2400 bps, the following standard is mandated:

- MIL-STD-188-182A, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997.

5.2.3.1.1.3 25kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service

For 25 kHz TDMA/DAMA service, supporting the transmission of voice at 2400, 4800, or 16000 bps and data at rates of 75-16000 bps, the following standard is mandated:

- MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, dated 2 December 1996.

5.2.3.1.1.4 Data Control Waveform

For interoperable waveform for data controllers used to operate over single access 5 kHz and 25 kHz UHF SATCOM channels, the following standard is mandated to provide a robust link protocol that can transfer error free data efficiently and effectively over channels that have high error rates:

- MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993.

5.2.3.1.1.5 DAMA Control System

For the minimum mandatory interface requirements for equipment that control access to DAMA UHF 5 kHz and 25 kHz MILSATCOM channels, the following standard is mandated:

- MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996.

5.2.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards

Communication services are provided via Earth, spot, and multi-beam array antennas. Data and voice services related to national military communication needs are carried via transponder channels. The six channels per DSCS III satellite vary in RF bandwidth from 50 to 85 MHz. Navy SHF satellite communication is used to carry tactical and strategic communication traffic to and from the fleet. Approved crypto is required to secure all RF links and measures are taken to prevent hostile analysis. The OM-55 modem is being phased out. The OM-73 and CQM-248A modems are the current technology. The Universal Modem System (UMS) is scheduled for Fleet Operational Test and Evaluation (FOT&E) in April 2000. The UMS offers the Navy a choice of Low Data Rate (LDR), up to 19.2 Kbps FSK and Medium Data Rate (MDR), 16 Kbps to 8.472 Mbps PSK service. Additional features include: the ability to use commercial satellites (C- and Ku-band), Frequency Division Multiple Access (FDMA), automatic RF power control, centralized control of UMS networks, and Over the Air Rekey (OTAR). Scheduled installations include command platforms, SHF SATCOM activities, Army, Air Force, United Kingdom and other NATO sites for extended interoperability.

Access http://www.jmcoms.org for more information about the Navy's SATCOM equipment development efforts.

5.2.3.1.2.1 Satellite Terminal Standards

To support minimum Radio Frequency (RF) and Intermediate Frequency (IF) requirements and ensure interoperability of SATCOM earth terminals operating over C-, X-, and Ku- band channels, the following standard is mandated:

- MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

Current draft standards for MILSATCOM are:

- MIL-STD-188-166 (Interface Standard, Interoperability and Performance of Non-Electronic Protective Measures (EPM) for SHF SATCOM Link Control Protocols and Messaging Standards),

- MIL-STD-188-167 (Interface Standard, Message Format for SHF SATCOM Demand Assignment), and
- MIL-STD-188-168 (Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications multiplexors and Demultiplexers).

5.2.3.1.2.2 Phase Shift Keying (PSK) Modems

For minimum mandatory requirements to ensure interoperability of PSK modems operating in Frequency Division Multiple Access mode, the following standard is mandated:

- MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995.

5.2.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards

World wide data and voice services are provided via two modes. Block I satellites offer Low Data Rate (LDR) service as follows. Low Hop Rate (LHR) at 75, 150, and 300 bps. High Hop Rate (HHR) provides 75 to 2400 bps data and 2400 bps voice service. Block II satellites add a Medium Data Rate (MDR) service, exchanging data at 4.8 Kbps to 1.544 Mbps. Navy EHF satellite communication is used to carry minimum essential communication traffic to and from the fleet. All RF links are secured by approved crypto. The system offers both jam resistance and LPI.

5.2.3.1.3.1 Low Data Rate (LDR) Links

For waveform, signal processing, and protocol requirements for acquisition, access control, and communication for low data rate (75-2400 bps) EHF satellite data links, the following standard is mandated:

- MIL-STD-1582D, EHF LDR Unlinks and Downlinks, September 30, 1996; with Notice of Change 1, dated 14 February 1997.

5.2.3.1.3.2 Medium Data Rate (MDR) Links

For waveform, signal processing, and protocol requirements for acquisition, access control, and communication for medium data rate (4.8 Kbps - 1.544 Mbps) EHF satellite data links, the following standard is mandated:

- MIL-STD-188-136, EHF MDR Uplinks and Downlinks, August 26, 1995; with Notice of Change 1, dated August 15, 1996, and Notice of Change 2, dated 14 February 1997.

5.2.3.1.4 Global Broadcast System (GBS)

Standards for GBS integration into the DISN have not been finalized, however proposals are in progress. GBS is patterned after Direct Broadcast Satellite (DBS), which is an example of Ku-band service concentrated in the more populated and affluent terrestrial areas of the Earth. It is a one-way broadcast that uses powerful uplink channels to make enough link budget that receivers (and antennae) can be quite small – approximately 18".

5.2.3.2 Commercial SATCOM

Terrestrial commercial carriers such as International Telecommunication Satellites (INTELSAT), Hughes Communication Services, and Orion, provide communication coverage for most sites on the Earth. Coverage by Earth coverage beams exists worldwide. Many carriers can provide higher

RF gain zone and spot coverage beams for most terrestrial sites. The higher RF gain allows the Earth terminal antenna to be smaller than that required for the same class of service in an Earth coverage RF beam. Both C- and Ku-band service are available world wide, but the Ku-band service is directed to service more populated terrestrial regions. The newest class of service, Direct Broadcast Satellite (DBS), is an example of Ku-band service concentrated in the more populated and affluent terrestrial areas of the Earth. Commercial carriers are capable of transferring many forms of data and protocol stacks by using proprietary protocols internal to the RF link. The transmit and receive sites perform the task of insuring continuity and delivery of the subject data.

The service provided is typically point-to-point and can be integrated by use of Point-to-Point Protocol (PPP) as a router-to-router interconnect. It is recommended that these channels be considered for integration after careful analysis of security.

The Commercial Satellite Communications Initiative (CSCI) has examined the vulnerabilities of using commercial satellites for military purposes. Currently completed studies include:

- "Project STARCROSS Commercial Satellite Vulnerability Study (U)", Report No. GX/S-733-93 of September 1993 for fixed and mobile satellite service provided by COMSAT, Hughes, and Loral Space Systems.
- "Project STARCROSS Mobile Satellite System Assessment: Phase II Results (U)", APL/TSD 34011 of December 1996 for mobile satellite service provided by Iridium.
- "Project STARCROSS Mobile Satellite System Assessment: Phase III Results (U)", APL/TSD 34672 of November 1997 for mobile satellite service provided by Globalstar

For release of documents, contact: Commander Naval Information Warfare Activity, 9800 Savage Road, Fort George Meade, MD 20755-6000

5.2.3.2.1 International Maritime Satellite (INMARSAT)

Since 1982 the International Maritime Satellite Organization (INMARSAT) has provided RF communication service to ocean regions and mobile users. The charter is to provide ship-to-shore and shore-to-ship telex and telephony for maritime customers, but recently land-mobile and air platforms have been added to the service.

INMARSAT system does not offer any communication protection and international treaty limits its use for purposes of war. According to an INMARSAT Consortium ruling (INMARSAT letter L303.0/vN/jr5376L of 8 November 1994), military use not involving armed conflict or any threat to or breach of peace is permitted. Also, military use of INMARSAT by UN peacekeeping or peacemaking forces acting under the auspices of the UN Security Council is permitted, even if engaged in armed conflict.

INMARSAT-B is the mandatory format for voice and data transfer. INMARSAT-C is used for Coast Guard navigation aides, as required. (Other INMARSAT systems are not recommended. INMARSAT-A is an expiring standard and is too easily compromised. INMARSAT-M lacks the communication quality offered by INMARSAT-B. Navigation aids via INMARSAT-C may become redundant by the year 2000.)

INMARSAT-B's internal link format is proprietary to INMARSAT which produces an effective data rate of 56 Kbps. The INMARSAT system does not offer any communication protection. Terminal manufacturers market terminals capable of operating in all existing INMARSAT environments. COMSAT Corp. in Clarksburg, MD at 301-428-2549, 2391, or 2660 has a current

list of certified INMARSAT terminal vendors. The information is also available via the World Wide Web at http://www.inmarsat.org/.

5.2.3.2.2 High Bandwidth Commercial SATCOM

The above-identified maritime transponders are not capable of a data transfer rate greater than 56 Kbps. Though high data rate service has been demonstrated from ships via terrestrial satellite carriers such as COMSAT, Hughes, and Orion no standards are currently designated. All demonstrations have been conducted close to terrestrial sites where high data rate service is offered, versus the middle of an ocean where the service is ultimately desired. As with any other installation of new equipment aboard a ship, a principle concern is location of the new above deck antenna(s).

5.2.3.2.3 Ku-Band Service

Data rates greater than 56 Kbps, as provided by INMARSAT L-band, are provided by terrestrial satellite service using C- and Ku-band RF links. Data transfer rates up to full motion video and beyond are capable within the satellite RF beam coverage foot print of the satellite. The issue of RF beam coverage is a principle issue relative to where this class of high data rate coverage is available.

High data rate service is often provided in 64 Kbps increments. Data-rates of 256 Kbps, 384 kbps, T1, E1, and 2.048 Mbps are popular transfer data rates. An Earth antenna as small as 2.4m is capable of receiving 24 Mbps data. Newer satellites transmitting to very small aperture terminal (VSAT) equipment with 18” diameter, receive-only antenna are capable of data-rates as high as 400 Kbps with average data transfer rates of 200 Kbps.

Four vendors of mobile satellite service use Low Earth Orbit (LEO) as this decreases the distance between uplink, satellite, and downlink stations with respect to geosynchronous satellites, enabling vehicle-mounted and handheld antennae as well as higher information transfer rates. Three of these vendors are considered “Big” because of the number of satellites in their constellations. The number of orbits of these satellites directly results in higher throughput capability as well as greater satellite coverage of the earth.

Globalstar is a constellation of bent-pipe satellites being launched by a consortium of Loral and Qualcomm. The system is known as a Big LEO system, is licensed by the Federal Communications Commission (FCC). Bent pipe means that the earth station (entry into the backbone network) and the mobile user must both be under the satellite footprint. The number of satellites and orbital configuration is such that satellites should be above the horizon at all times in temperate and equatorial areas (Globalstar does not provide polar coverage). Because Globalstar was designed with trunked voice applications in mind, media access is point-to-point at rates of approximately 19.2 Kbps (Rate Set 2), 9.6 Kbps, 4.8 Kbps and 2.4 Kbps. The user is provided a handset similar to that in any telephone cellular system. Predicted weight is 16 oz with a desired lifetime of 24 hours standby-time and 2 hours talk-time.

Iridium is a constellation of satellites with crosslinks that is being launched by a consortium led by Motorola. This system is known as a Big LEO and is licensed by the FCC. With satellite crosslinks, the mobile user and terrestrial network entry can be anywhere. Iridium's orbital configuration is near-polar so complete global coverage (including Polar Regions) can be expected. Because Iridium was designed with trunked voice applications in mind,

media access is point-to-point at rates of approximately 9.6 Kbps. The user is provided a handset similar to that in any telephone cellular system. Predicted weight is 16 oz with a desired lifetime of 24 hours standby-time and 2 hours talk-time.

Orbcomm is a constellation of satellites launched by Orbital Sciences Corporation. This system is known as a Little LEO and is licensed by the FCC. It is a data-only, store-and-forward system designed to relay small e-mail messages from users to e-mail gateways, for dispatch into the Internet. The mobile user is provided an antenna and module that connect to a host computer via RS-232. Demonstrated systems have been designed for automobile installation and weigh less than 5 pounds complete.

Teledesic is an emerging infrastructure of satellites expected to reach initial operational capability in 2002. It is a consortium with support from AT&T, McCaw and Microsoft. The 288 satellites are planned into a near-polar low earth orbit, so complete earth coverage, including Polar Regions, can be expected. Teledesic has satellite crosslinks, and an order of magnitude higher capacity than the other big LEOs. While the interface to the terrestrial internet is as yet undefined, the term 'Internet' appears prominently in Teledesic's business plan. Teledesic plans to develop alliances with service provider partners in host countries worldwide, rather than marketing directly to end users. The Teledesic system is designed to provide up to 64 Mbps on the downlink and up to 2 Mbps on the uplink. Broadband terminals will offer 64 Mbps of two-way capacity. Teledesic plans to be operational by the year 2002.

5.2.3.3 Line-of-Sight (LOS) Radio Communications

5.2.3.3.1 Military Communication Systems

5.2.3.3.1.1 High Frequency (HF) and Automatic Link Establishment (ALE)

For both ALE and radio subsystem requirements operating in the HF bands, the following standard is mandated:

- MIL-STD-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, September 15, 1988; with Notice of Change 1, dated 17 June 1992, and Notice of Change 2, dated 10 September 1993.

5.2.3.3.1.1.1 Anti-jamming Capability

For anti-jamming capabilities for HF radio equipment, the following standard is mandated:

- MIL-STD-188-148A, Interoperability Standard for Anti-Jam Communications in the HF Band (2-30 MHz), 18 March 1992.

5.2.3.3.1.1.2 Data Modems

For HF data modem interfaces, the following standard is mandated:

- MIL-STD-188-ll0A, Data Modems, Interoperability and Performance Standards, 30 September 1991.

5.2.3.3.1.2 Very High Frequency (VHF)

For radio subsystem requirements operating in the VHF frequency bands, the following standard is mandated:

- MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985.

5.2.3.3.1.3 Ultra High Frequency (UHF)

For radio subsystem requirements operating in the UHF frequency bands, the following standard is mandated:

- MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989.

5.2.3.3.1.3.1 Anti-jamming Capability

For anti-jamming capabilities for UHF radio equipment, the following standard is mandated:

- STANAG 4246, Edition 2, HAVE QUICK UHF Secure and Jam-resistant Communications Equipment, June 17, 1987; with Amendment 3, dated August 1991.

5.2.3.3.1.4 Super High Frequency (SHF)

For radio subsystem requirements operating in the SHF frequency bands, the following standard is mandated:

- MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, dated 28 July 1992.

5.2.3.3.2 Commercial Non-Satellite Radio Communication Systems

5.2.3.3.2.1 Personal Communications Services (PCS)

PCS will support both terminal mobility and personal mobility. Personal mobility allows users of telecommunication services to gain access to these services from any convenient terminal with which they choose to associate themselves. To support personal mobility, the network must be able to distinguish between terminal and personal identifiers; to keep track of current user-terminal associations, user locations, services authorized to the user, and service capabilities of the terminals. Either wireline or wireless terminals may provide personal mobility. Terminal mobility is based on wireless access to the Public Switched Telephone Networks (PSTN). Wireless access standards will govern the protocols and procedures for establishing connections among mobile terminals and between them and fixed terminals of a switched network (or mobile terminals of a different cellular system). IS-41, the current standard within the United States, provides this capability and is compatible with the existing signaling and numbering schemes used in the PSTN.

5.2.3.3.2.2 Mobile Cellular Communications

Mobile cellular radio can be regarded as an early form of “personal communications service.” It allows subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. Two methods for digital access have emerged, TDMA, and Code Division Multiple Access (CDMA). In North America the standards for TDMA and CDMA are IS-54 and IS-95. Both of these standards use IS-41 as the standard signaling protocol.

5.2.3.3.2.3 Future Public Land Mobile Telecommunications Systems (FPLMTS) standards

The ITU is now working on a third-generation standard for FPLMTS. The aim of this effort is to achieve better compatibility among the various cellular systems such that, by the beginning of the next century, universal global access supporting terminal mobility becomes a reality. The

document now emerging from this effort shall be used as guidance for implementing global terminal mobility.

5.3 Internetwork Protocols

Layers 3 and 4 of the OSI Reference Model (Figure 5-7. ISO/OSI Model Layers 3 and 4) describe the network and transport layers, respectively. Transmission Control Protocol/Internet Protocol (TCP/IP) (defined later) falls into this area. There is currently an active debate within the industry on whether to strictly follow the traditional Internet model in which all data is broken into connectionless packets (called “datagrams”) or allow for connection-oriented streams as in ATM (defined below).

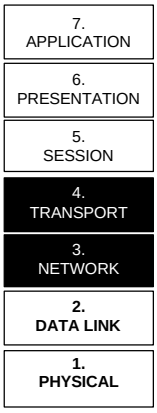

Figure 5-7. ISO/OSI Model Layers 3 and 4

When following the connectionless model, each datagram is handled independently. A decision on how to route information from one point to another is made on each and every datagram. The benefits are that one can be completely independent of the data link layer from one segment to another as packets cross the network. Also, as intermediate links come and go, the independent routing of each datagram provides a good chance that an alternate path will be found on the fly. The disadvantage is that processing, sometimes significant, must occur on each and every datagram, i.e., the “n”th datagram has no knowledge of the path that the “n-1”st datagram took.

The connection-oriented, or “virtual circuit” model requires that one establish a virtual circuit between two points via a call-setup procedure. Once the circuit is created, information can flow along this predefined path without the need to examine the individual data elements. Each virtual circuit can be created with its own quality-of-service requirements (bandwidth, minimum delay, bumping priority, etc.) By allowing a connection-oriented “virtual circuit”, one can pay the processing overhead once in performing the “call setup” to establish the path, then have all subsequent data follow the original path with minimal processing, i.e., higher bandwidth. A disadvantage is that one must recreate the virtual circuit upon any given link failure.

A crude analogy can be made between postal mail and a telephone call. With the postal mail example, a data set too large to fit into one envelope can be broken up into many, separately addressed envelopes (connectionless datagrams). Each envelope can then be transported by independent means from the source to the destination. If, however, a phone call were placed (connection-oriented virtual circuits), the data would travel the same deterministic path from the source to the destination.

This arguments of this debate are much more complex than the above and are beyond the scope of this document. The most likely outcome will be a hybrid set of standards that allow for both environments. One of the major goals of this chapter is to provide a single core infrastructure that will handle both types of data flow. Provisions are made for both implementations to simultaneously exist and pass data back and forth. For example, a low-end client connected to an Ethernet segment generating IP datagrams should be able to simultaneously communicate with a peer operating in the same state as well as with a server that is directly connected to other servers via ATM. Also, a real-time data stream (such as a VTC session or video broadcast) that does not implement IP will be able to share the same core backbone.

Best Practices

ATM from the desktop through the WAN is recommended to the extent that application interoperability and cost will allow. Where ATM is not yet feasible, continued use of Transmission Control Protocol/Internet Protocol (TCP/IP) is recommended for shared media networks (LANs) Point-to-Point (PPP) protocol is recommended for point-to-point links and WANs.

LAN configurations for the backbone, servers, mission critical appliances, and non-mission critical appliances should be consistent throughout the information system domain. Mixing of different protocols on like architectural components (e.g., all non-critical appliances) is not permitted except temporarily during the migration to an advanced protocol.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
Novell's IPX	ATM	ATM	ATM	ATM	IPv6
Banyan's Vines	IPv4	IPv4	IPv4	IPv4	
AppleTalk	TCP	TCP	TCP	TCP	
DecNET/LAT	ppp	ppp	ppp	ppp	
Activities, Platforms, Operational Environments		All. ITSC managed			

Table 5-5. Network and Transport Layer Recommended Implementations

5.3.1 ATM

Asynchronous Transfer Mode (ATM) is a connection-oriented transport protocol that collapses many of the layers of the OSI model.

Briefly, ATM uses "virtual circuits". (The virtual circuits can be established in advance (Permanent Virtual Circuits, or PVCs) or dynamically on demand (Switched Virtual Circuits, or SVCs).) ATM Virtual Circuits (VCs) are based on the concept of Asynchronous Time Division Multiplexing, ATDM. Unlike traditional TDM systems in which each multiplexed VC is given a predetermined time slot, ATDM fills the "next" available time slot with data from the "next" available VC. For example, given "n" VCs, traditional TDM would uniformly transmit one fixed-length data unit (called a "cell") from one VC to the next. After one time period, the first cell of all "n" VCs would have been transmitted. If no cells were ready from a particular VC, a "null" cell would be inserted into the multiplexed output stream. (The receiving device would properly identify these "null" cells and discard them.) With ATDM, however, the next cell could come from any VC. For example, if there were two VCs, one of which had twice the bandwidth on the other, then the higher-bandwidth VC would transmit two cells for every cell of the lower-bandwidth VC. Also, if a higher-priority VC had a cell ready, it would be transmitted before a lower-priority VC – even if the former was at a lower bandwidth.

ATM Virtual Circuits can support a number of service classes based on the traffic type, each with an associated set of Quality of Service (QoS) parameters. Example service classes are as follows:

- Constant Bit Rate (CBR), used for circuit emulation and flows which have a constant data rate
- Variable Bit Rate (VBR) for flows which are bursty in nature (further QoS parameters for this traffic type are Peak Cell Rate (PCR) for maximum burst rate and Sustained Cell Rate (SCR) for average rate)
- Available Bit Rate (ABR) for flows which dynamically negotiate their PCR and SCR values
- Unspecified Bit Rate (UBR) for "best-effort" service.

Some applications are obviously linked to particular service class. A 64 Kbps voice circuit is best carried as a CBR stream but voice which is compressed and has silence-suppression enabled can either be VBR or UBR, depending on the robustness of the algorithm. How applications map to the different service classes is evolving.

By allowing VC cells to enter the multiplexed stream under individually controllable conditions, i.e., service classes, one could enforce the QoS for a particular VC. A high-bandwidth VC would have more access to a trunk than a lower-bandwidth VC. Similarly, a high-priority VC has head-of-the-line privileges over a lower-priority VC.

ATM has no length or time-delay constraints. As a result, it is applicable to the LAN as well as the WAN. Further, ATM is a technology that can cut through many of the OSI layers. At the application layer, one could open a virtual circuit between two workstations using all layers of the OSI 7-layer model. Once the circuit was established, however, data could simply flow from the application (layer 7) to the data link layer (layer 2) – without passing through the intermediate layers (3 through 6). (In IP, all data is broken into datagrams, each of which passes through all layers.) ATM can simultaneously support applications whose data does not easily fit the 7-layer model (VTC, voice, real-time data streams, etc.). Finally, VC cells can be replicated at convenient points along the network and sent to multiple users. A single source can transmit one stream to multiple users. If the users are a significant distance apart, say across the country, the stream is not duplicated until the last possible point. This is very efficient in bandwidth utilization, especially for multicast.

For the above reasons, ATM is a technology that must be considered in future systems. It continues to gain acceptance in WAN technology and can offer hundreds and thousands of Mbps rates in the LAN.

As a transition phase, most computer applications implement IP over ATM as opposed to TCP over ATM (IP and TCP are discussed below). As a result, many of today's applications create datagrams within the operating system and transmit those individual datagrams via ATM. As applications' needs warrant, they can be migrated over to ATM such that many of the OSI layers are never traversed, resulting in higher efficiency.

5.3.2 Network Layer

This section provides a discussion of the Network Layer as defined by the OSI Reference Model. The network layer provides the interface between the lower layer protocols and the transport layer protocols and the means for concatenating multiple network segments into a seamless whole. The recommended network layer protocol is the Internet Protocol or IP. This section also addresses protocols that support and integrate IP with the lower layer protocols.

Needs:

- Each protocol that runs over a network requires overhead. This overhead is most commonly manifested in terms of bandwidth used (e.g. to pass routing table updates) and in terms of administrative time and expense. This set of standards is intended to converge to a single set of protocols that exacts this overhead tax but once.
- The IP protocol base outlined here allows one option towards a forward evolution to a multicast set of protocols as they develop in the industry.

5.3.2.1 Internet Protocol

The Internet Protocol (IP), also referred to as the Internet Protocol Version 4 (IPv4), refers to an unreliable, connectionless, datagram service. The IP is defined by the Internet Architecture Board (IAB) Standard 5.

- IAB Standard 5 is comprised of the IP specification (RFC 791 as amended by RFCs 950, 919, and 922) and integral support protocols
- Internet Control Message Protocol (ICMP), as specified in RFC 792
- Internet Group Multicast Protocol (IGMP), as specified in RFC 1112.

The IP, including ICMP and IGMP, is mandated in the Joint Technical Architecture.

Multicast IP provides the ability to send data to multiple destinations without requiring datagrams to transit any link more than once. It is widely supported by routers and some end systems and should be introduced incrementally. IPv6 is the next generation of Internet Protocol and will be introduced incrementally into the Internet over the next several years. IPv6 incorporates the Multicast IP features as well needed security features. The Naval infrastructure should incrementally evolve toward IPv6 as there are very few products implementing IPv6 and its deployment has been much delayed.

5.3.2.2 Address Resolution Protocol

An address resolution protocol (ARP) is used to determine a data link layer address based upon a specific network layer address. The ARP capability is required for each data link layer supported.

- IAB Standard 36, specified in RFC 1390, defines the transmission of IP and ARP for FDDI networks.
- IAB Standard 37, specified in RFC 826, defines the ARP for Ethernet networks.
- The ARP for ATM is dependent upon the adaptation protocol support capability (i.e., LANE for Ethernet, RFC 1577 for Classical IP over ATM, MPOA).
- RFC 1122, “Requirements for Internet Hosts – Communication Layers”, part of the IAB Standard 3, provides additional guidelines for the ARP.

IAB Standard 37 is mandated in the Joint Technical Architecture.

5.3.2.3 Point-to-Point Protocol

The Point-To-Point Protocol (PPP) provides a protocol independent transport service for datagrams over point-to-point links. Examples of point-to-point links include dial-in from outside the network, router-to-router interconnect, and many satellite lines (by virtue of their engineering). The PPP is Internet Architecture Board (IAB) Standard 51. IAB Standard 51 is specified in RFC 1661 and RFC 1662. Additional guidelines for the PPP are provided in RFC

1122, “Requirements for Internet Hosts --Communication Layers”, part of the IAB Standard 3. The PPP is mandated in the Joint Technical Architecture.

Existing SLIP (Serial Line IP) connections should be incrementally phased out and new SLIP connections should not be supported as PPP is a complete next-generation superset to SLIP and is widely supported by vendors.

5.3.2.4 Obtaining IP Addresses

Official (registered) IP addresses for the U.S. Navy ships and shore commands can be obtained from the Naval Computer and Telecommunications Station (NCTS) Pensacola, Florida at (COMM) 850-452-3501, (DSN) 922-3501. A convenient and efficient method for all ships and unclassified shore commands is the use of the on-line Navy IP Network Number Registration page whose URL is http://www.netreg.navy.mil/. The e-mail address for ships is shipreg@ncts.navy.mil and for shore commands is netreg@ncts.navy.mil. The method for classified shore commands is an on-line Navy IP Network Number Registration page whose URL is http://www.netreg.navy.smil.mil/. The e-mail address is netreg@ncts.navy.smil.mil.

IP addresses are officially tracked and assigned only to the level of a Class C address. The use of subnet masking to subdivide Class C addresses is a matter for local shipboard network administration.

5.3.2.5 Obtaining NSAP Addresses

ATM networks require Network Service Access Point (NSAP) addresses. While the format for NSAP addresses is well defined, the mechanism for obtaining these addresses and properly constructing an ATM topology is still being developed. DISA will administer the DoD NSAP addressing plan and the DON should obtain its addresses from it. NCTS Pensacola is making preparations to provide NSAP addresses to complement IP network address service. The DISA addressing plan is geographically-based for global scalability. It is lacking a robust scheme for deployed forces and mobile users because supporting standards are not yet mature. In the short term, DISA will coordinate with DON users to assign addresses that can be readvertised as deployable forces move. The two options, to be resolved on a case-by-case basis, are to use a geographic address or a reserved globally unique address. In either case, DISA will move the address advertisement within their network as the deployable force moves. When an adequate standards-based mobile protocol exists, DISA will adopt it. A more complete NSAP addressing scheme will be provided in a future version of the ITSG.

5.3.2.6 Use of Proprietary Network Layer Protocols

Proprietary network layer protocols such as Novell’s IPX or Banyan’s Vines IP should not be planned for new systems. However, interoperability between IPX or Vines IP and standard IP will require a network layer gateway and should preferably be avoided.

5.3.3 Transport Layer

This section provides a discussion of the Transport Layer as defined by the OSI Reference Model. The transport layer provides the interface between the network layer protocol and the upper layer protocols. It operates between consenting end systems across the unreliable networking infrastructure to enforce a defined quality of service. The two dominant transport layer protocols used in conjunction with the IP are the Transmission Control Protocol (TCP) and the User

Datagram Protocol (UDP). A third protocol specified but not in use is the Real-time Transport Protocol (RTP).

5.3.3.1 Transmission Control Protocol

The Transmission Control Protocol (TCP) provides a reliable, connection-oriented (end-to-end) transport service used with IP. It supports many application layer protocols such File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) for e-mail and Hypertext Transfer Protocol (HTTP). TCP, while a powerful and ubiquitous protocol, has some limitations that are important to the Naval community. TCP is a unitcast protocol – it does not support multicast. Also, except for error-free transmission (at the application layer), TCP has no precedence or QoS mechanisms. The TCP is Internet Architecture Board (IAB) Standard 7. IAB Standard 7 is specified in RFC 793. Additional guidelines for the TCP are provided in RFC1122, "Requirements for Internet Hosts -- Communication Layers", part of the IAB Standard 3. Flow control requirements are as specified in RFC 2001. The TCP is mandated in the Joint Technical Architecture.

5.3.3.2 User Datagram Protocol

The User Datagram Protocol (UDP) provides a connectionless, datagram transport service used with the IP. UDP uses whatever quality-of-service is inherent in the underlying structure. For example, if a datagram is lost because of a router overflow, UDP will not detect the loss nor require a retransmission. The UDP is Internet Architecture Board (IAB) Standard 6. IAB Standard 6 is specified in RFC 768. Additional guidelines for the UDP are provided in RFC 1122,"Requirements for Internet Hosts -- Communication Layers", part of the IAB Standard 3. The UDP is mandated in the Joint Technical Architecture.

5.3.3.3 Real-Time Transport Protocol

The Real-time Transport Protocol (RTP) provides end-to-end transport for applications with real-time characteristics. Examples of such applications include interactive audio and video. The RTP was developed by the IETF and is specified in RFC 1889. RTP usage is not currently widespread.

5.4 Routing and Mobility Protocols

Best Practices

Use Open Shortest Path First version 2 (OSPF 2) for the interior gateway protocol (IGP) and Border Gateway Protocol version 4 (BGP 4) for the exterior gateway protocol (EGP). Use Private Network-to-Network Interface (PNNI) for ATM networks. Use Classless Inter Domain Routing (CIDR) to the maximum extent possible to simplify routing configured -- obtaining IP addresses from NCTS Pensacola with CIDR implementation. Use Dynamic Host Configuration Protocol (DHCP) to provide mobility and conservation of IP addresses.

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
IPNetBEUI LAT IGRP RIP DVMRP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	OSPF2 for IP IGP BGP4 for IP EGP PNNI for ATM DHCP	MOSPF PIM MBGP
Activities, Platforms, Operational Environments	All. Managed by the ITSC.				

Table 5-6. Network Routing Protocol Recommended Implementations

5.4.1 Routing

Routing protocols are historically defined for IP datagrams, i.e., how does one “route” a datagram from one network (or subnetwork) to another.

Any device is considered a router if it interconnects one or more networks (or subnetworks) and makes forwarding decisions based upon network layer protocol addresses contained in the IP datagrams or ATM call-setup requests it receives. (When only ATM call-setup requests are involved, this function is performed on a switch.) This section specifies a set of routing information and supporting protocols that allows routers and switches to work together and avoids paying certain overhead costs more than once.

The IETF has developed a document which outlines requirements for Internet Protocol (IP) routers, RFC 1812, “Requirements for IP Version 4 Routers.” This document outlines the requirements for support of the IPv4, including support for ICMP, IGMP, ARP, and PPP; as described above. In addition, the RFC provides guidance for routing protocol support and addressing. These standards are consistent with RFC 1812.

The ATM Forum provides standards for the Private Network-to-Network Interface (PNNI) .

5.4.1.1 Addressing

Devices providing the routing function should support both the classical (or hierarchical) IP addressing model and Classless Inter Domain Routing (CIDR). The classical (or hierarchical) interpretation of the Internet address space is that of a 32-bit address partitioned into a network number and a host number; where the network number identifies a hierarchy of addresses and can be further partitioned into subnetworks. CIDR replaces the concept of address classes. The key concepts behind CIDR are:

- The addresses are assigned based upon topology
- Routing protocols are capable of aggregating network layer reachability information
- Use of consistent (longest match) forwarding algorithm.

As part of CIDR, the interpretation of the 32-bit IP address was revised. Instead of fixed-size network and host numbers for the various classes; the address specification refers to a “network

prefix" and a "host prefix." The network prefix is a contiguous string of bits at the most significant portion of the address. The use of the longest match-forwarding algorithm permits more efficient allocation and use of the 32-bit IP address space. CIDR is specified in RFC 1519.

5.4.1.2 Routing Protocols

A routing protocol addresses the need to exchange network reachability information with other routers and end systems. Two basic types of routing protocols are generally used. An interior gateway protocol (IGP) exchanges routing information with other routers, typically within the same administrative domain referred to as an Autonomous System (AS). An exterior gateway protocol (EGP) exchanges routing information with routers that are external to the administrative domain (or between "autonomous systems").

ATM switches exchange routing information using PNNI.

Support for the following routing protocols will provide interoperability with existing and planned systems.

5.4.1.2.1 Routing Information Protocol

The Routing Information Protocol (RIP) is a legacy IGP. Although RIP is identified as IAB Standard 34, it has recently been moved to historical status. The RIP should only be used to support Legacy LAN networks. Support for RIP can be accomplished by the implementation specified in RFC 1058. A second alternative for the support of RIP in legacy systems is the implementation of RIP Version 2 (RIPv2). Although interoperability issues can arise, the RIPv2 specification, RFC 1723, does address interoperability with legacy RIP. RIP should be avoided. (It is included in these discussions because a significant number of equipment manufacturers and users still use this protocol.)

5.4.1.2.2 Open Shortest Path First Version 2

The Open Shortest Path First Version 2 (OSPF2) is also an IGP. It is specified in RFC 1583. RFC 1812, "Requirements for IP Version 4 Routers" recommends the use of OSPF2 for the IGP. OSPF2 is mandated in the Joint Technical Architecture.

5.4.1.2.3 Distance Vector Multicast Routing Protocol

Multicast routing is an evolving technology within the IETF and many vendors are waiting for standards to solidify before providing an implementation. The Distance Vector Multicast Routing Protocol (DVMRP) is the most widely supported of the multicast routing protocols. It was also the basis for much of the Multicast Backbone (MBONE) capability and research efforts involving multicast technology. DVMRP has evolved from its version initial specification (RFC 1075) to its present protocol specification documented in draft-ietf-idmr-dvmrp-v3-04.txt (an Internet Draft). Because it has scaling issues and is not widely supported by vendors, it is not a recommended protocol.

5.4.1.2.4 Border Gateway Protocol Version 4

The Border Gateway Protocol Version 4 (BGP-4) is the EGP recommended in RFC 1812, "Requirements for IP Version 4 Routers". BGP-4 is specified in RFC 1654. BGP-4 is mandated in the Joint Technical Architecture.

5.4.1.2.5 Protocol Independent Multicast

Protocol Independent Multicast (PIM) is a new IETF internal routing standard which is gaining wide support and is therefore in the emerging category.

5.4.1.2.6 Private Network-to-Network Interface

Multicast Border Gateway Protocol (MBGP) is an extension of the exterior routing protocol BGP. It is an emerging standard.

5.4.1.2.7 Private Network-to-Network Interface

There are a number of Private Network-to-Network Interface protocols for ATM (PNNI). All but one, ATM Forum PNNI, is proprietary. A number of manufacturers now offer ATM Forum PNNI. Version 1.0, or Phase 1, is recommended as the preferred standard.

5.4.1.3 Use of Non-Routable Protocols

The use of non-routable protocols such as NetBEUI, LAT, etc., is discouraged. Such protocols do not scale and introduce great difficulties in trying to interconnect multiple networks.

5.4.2 Mobile Addressing

Mobility is currently defined as transportability, i.e., moving a network node from one subnetwork to another but *not* requiring connectivity during the move. This is evolving and will eventually provide for true mobility, i.e., remaining connected during a move. (It is interesting to note that in the wireless area, LEO satellites have the reciprocal effect of mobility, namely, they will be moving so fast (with respect to the user) that the network will move even if the user doesn't. The same protocols can be used in either case.)

5.4.2.1 Dynamic Host Configuration Protocol (DHCP)

DHCP supports several features useful to the Naval network:

- Automatic assignment of IP addresses and configuration data such as netmask and Domain Name System (DNS) server
- Assignment of addresses that are actually used, resulting in economy of IP addresses (unused addresses are reclaimed for reuse)
- Ease of system administration due to automation and ability to administer these details from the server rather than the client.

While DHCP is not intended to support mobile users, it is also valuable in supporting laptop plug in at remote locations. Notably, DHCP actually assigns a new IP address to the end system so the DNS database must change (which requires some settling time) before full service catches up.

5.4.2.2 Mobile IP

Mobile IP is a developing standard within IETF that is designed to support mobile users that move from one domain to another. It operates on a set of home and foreign agents that keep track of forwarding data for a user. In the case of Mobile IP, the end system IP address does not change, so there is no DNS impact.

Mobile IP has considerable value for situations requiring mobile and deploying staffs.

Warning. Both the DHCP and Mobile IP assignment databases contain data that could yield order of battle intelligence so they should be deployed and managed with appropriate attention to security.

5.4.2.3 Mobile NSAP

The need for mobile ATM is just as relevant as for mobile IP. Work is underway to provide an addressing scheme in which one can move their NSAP address as one would move their cellular telephone.

5.5 Quality-of-Service

Best Practices

ATM is the preferred network protocol because of its versatility and its ability to support Quality-of-Service (QoS).

Recommended Implementations

	Current ITSG	Projected ITSG			
Not Recommended	**1999**	**2000**	**2001/2002**	**2003/2004**	**Emerging**
	ATM	ATM	ATM	ATM	RSVP for TCP/IP
Activities, Platforms, Operational Environments		All. Managed by the ITSC.			

Table 5-7. Quality of Service Recommended Implementations

5.5.1 Description

Quality-of-Service (QoS) is that which provides a level of data transfer which systems can rely on to meet their design goals. For example, if a given application requires a certain minimum bandwidth in which to function properly, it requires that *every* component from the physical media through the operating system guarantee that bandwidth. There are many QoS parameters such as minimum bandwidth, maximum bandwidth, average bandwidth, minimum delay (latency), jitter (delay variation), preemption priority, maximum interrupt time, etc.

At a minimum, the QoS capability of subsystems must be known and bounded so that applications can be designed accordingly. At best, an application will be able to request a particular QoS and receive a high-level of assurance that this “contract” between itself and the lower levels will be honored.

In the network, the first 4 layers of the OSI model must supply QoS. In particular, the bandwidth and delay characteristics of the medium through the processing of data packets and state changes (updating routing information) apply.

QoS is generic in that it affects all communities. DoD is unique in that command and control requires a preemption capability in case of national emergency. DON has additional requirements on board ships and aircraft in that the RF bandwidth to/from these platforms will always be

limited, i.e., one simply cannot supply all the bandwidth a ship/aircraft requires. Managing such limited-bandwidth connections is a challenge.

5.5.2 State

There are three levels of QoS in existence today:

- Best effort
- Provisioned service
- On-demand, negotiated service

5.5.2.1 Best Effort

Best effort QoS is exemplified both by the traditional record message system and by the Internet. As demand exceeds supply, queues form and delays are incurred. As the queues continue to build, a point is reached when the buffers begin to overflow and message traffic is rendered useless due to late delivery or loss. This loss of traffic tends to be non-discriminatory – all users get degraded service.

5.5.2.2 Provisioned Service

Provisioned service is what is used to provide WAN links such as DS-1 and DS-3. The customer requests a dedicated circuit at a particular rate between two points. This circuit is established and is guaranteed to be “up” and under full control of the user. While this is guaranteed, it can become prohibitively expensive. For example, if a user needs an OC-3 peak (155 Mbps) for only short periods throughout the day, one must pay for the entire circuit 24 hours per day.

5.5.2.3 On-Demand, Negotiated Service

On-demand, negotiated service is analogous to the telephone system. Once places a call on demand. If the call goes through, the user is happy. If, however, it is blocked (a busy signal), the user is not happy. Also, an existing call may be dropped if a higher-priority call comes through (FLASH, for example). In modern networks there are more than two levels (call gets through or doesn’t). Usually virtual circuits are established but IP datagrams or ATM cells are individually delayed, or even blocked. Most applications will retransmit and the user simply sees a momentary delay.

5.5.2.4 Summary

All models are of value in the military. Under best effort, if the occurrence of delay is visible to users, it becomes a feedback mechanism that assumes that users will discipline themselves to restrict traffic to that essential to business. This model tends to be fairly resilient, albeit frustrating, under stress.

The provision service provides the guaranteed QoS that critical command and control systems need. For example, data may have completely lost its value if it arrives too late. The class of service, however, is expensive and cannot respond quickly to changing requirements.

The on-demand, negotiated model is very important in that it can respond quickly to changes in requirements.

QoS features in various network protocols are designed to meet various facets of one of these models. But the problem is complex – it pervades every layer of the ISO Reference Model. For example, it is of no use to have the network provide a guaranteed minimum delay if the operating system cannot also honor this "contract." Also, other factors greatly affect the network's ability to provide a given level of QoS. For example, the amount of interleaving in forward error correction (physical), packet size and media access method (data link), router and switch configuration (network) and transport protocol error correction doctrine (transport) are all pertinent examples.

The various recommended protocols in this chapter address different aspects of the QoS problem:

- Homogenous ATM networks (LANs or WANs) can offer QoS guarantees to the workstation.
- Standards work in the ATM Forum is proceeding to allow applications to specify QoS parameters to the network.
- Within single segment LANs, FDDI offers deterministic service. Ethernet provides a best-effort service. Neither can offer QoS guarantees across a WAN.
- Standards work in the IETF is proceeding to offer both preferential non-deterministic service and bounded delay service upon implementation of RSVP (Resource Reservation Protocol). In order to operate to scale, all routers between end systems must be RSVP-capable and the end systems must be RSVP-protocol aware in order to request resources from the routers.

The mechanisms to control quality of service in the network in its larger dimension (more than one segment) are still maturing. Further, the doctrine and management structure to control the mechanisms when they are available is evolving. Nonetheless, we should be looking to incorporate tools, as they become available.

5.6 References

5.6.1 Standards and Specifications Resources

Physical and Data Link for the LAN

Naval Sea Systems Command (NAVSEA) document: "NIIN IPT Near term Guidance for Shipboard Networks", 11 November 1997

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 802.1d, Spanning Tree for Network Reconfiguration

Laubach (Hewlett Packard); ,"Classical IP over ATM" (RFC 1577); January 1994; ftp://ftp.isi.edu/in-notes/rfc1577.txt (23 May 1998)

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 802.1Q, "Draft Standard for Virtual Bridged Local Area Networks"

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 802.10 "Link-layer Standard for Interoperable LAN Security (SILS)"

Institute of Electrical and Electronics Engineers (IEEE) specification; IEEE 802.11-1997 "Wireless LAN Media Access Control (MAC) and Physical Layer (PHY)"

Institute of Electrical and Electronics Engineers (IEEE) standard; IEEE 801.1p, Standard for Local and Metropolitan Area Networks – Supplement to Media Access Control (MAC) Bridges: Traffic Class Expediting and Dynamic Multicast Filtering

ATM Forum specification, af-uni-0010.002: "ATM User-Network Interface Specification V3.1, 155.52 Mbps Optical Interface", 1994, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-phy-0046.000 662.08 Mbps Optical Interface, January 1996; www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-phy-0054.000 44.736 Mbps Coax Interface, March 1996, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

Physical and Data Line Protocols for Radio Communications

Department of Defense (DOD) MIL-STD-188-181A, Interoperability Standard for Single Access 5 kHz and 25 kHz UHF Satellite Communications Channels, 31 March 1997

Department of Defense (DOD) MIL-STD-188-182A, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 31 March 1997

Department of Defense (DOD) MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, dated 2 December 1996

Department of Defense (DOD) MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993

Department of Defense (DOD) MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

Department of Defense (DOD) MIL-STD-188-166 (Interface Standard, Interoperability and Performance of Non-Electronic Protective Measures (EPM) for SHF SATCOM Link Control Protocols and Messaging Standards)

Department of Defense (DOD) MIL-STD-188-167 (Interface Standard, Message Format for SHF SATCOM Demand Assignment)

Department of Defense (DOD) MIL-STD-188-168 (Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications Multiplexors and Demultiplexers)

Department of Defense (DOD) MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995

Department of Defense (DOD) MIL-STD-1582D, EHF LDR Unlinks and Downlinks, September 30, 1996; with Notice of Change 1, dated 14 February 1997

Department of Defense (DOD) MIL-STD-188-136, EHF MDR Unlinks and Downlinks, August 26, 1995; with Notice of Change 1, dated August 15, 1996, and Notice of Change 2, dated 14 February 1997 Katz (Cisco); "Transmission of IP and ARP over FDDI Networks" (IAB Standard 36/RFC 1390), January 1993; ftp://ftp.isi.edu/in-notes/rfc1390.txt (23 May 1998)

Department of Defense (DOD) MIL-STD-188-141A, Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, September 15, 1988; with Notice of Change 1, dated 17 June 1992, and Notice of Change 2, dated 10 September 1993

Department of Defense (DOD) MIL-STD-188-148A, Interoperability Standard for Anti-Jam Communications in the HF Band (2-30 MHz), 18 March 1992

Department of Defense (DOD) MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985

Department of Defense (DOD) MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989

Department of Defense (DOD) MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, 28 July 1992

North American Treaty Organization (NATO) standard: STANAG 4246, "HAVE Quick UHF Secure and Jam-resistant Communications Equipment", Edition 2, 17 June 1987; with Amendment 3, August 1991, /www-library.itsi.disa.mil/org/stanag/4246.htm (23 May 1998)

Space and Naval Warfare Systems Center (SPAWAR) Joint Maritime Communications System (JMCOMS) web page: www.jmcoms.org (23 May 1998)

Teledesic Corporation web page: www.teledesic.com (23 May 1998)

Inmarsat web site: www.inmarsat.org (23 May 1998)

Internet Protocols

Postal (USC ISI); "Internet Protocol" (RFC 791), September 1981, http://info.internet.isi.edu:80/in-notes/rfc/files/rfc791.txt (23 May 1998)

Postal (USC ISI); "Internet Control Message Protocol (ICMP)" (RFC 792); September 1981; ftp://ftp.isi.edu/in-notes/rfc792.txt (23 May 1998)

Postel (USC ISI); "Transmission Control Protocol" (RFC 793/IAB Standard 7) September 1981; ftp://ftp.isi.edu/in-notes/rfc793.txt (23 May 1998)

Plummer (MIT) "An Ethernet Address Resolution Protocol" (IAB Standard 37/RFC 826) November 1982; ftp://ftp.isi.edu/in-notes/rfc826.txt (28 May 1998)

Mogul (Stanford) "Broadcasting Internet Datagrams in the Presence of SubNets" (RFC 922), October 1984; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc922.txt (23 May 1998)

Mogul (Stanford), Postal (USC ISI); "Internet Standard Subnetting Procedure" (RFC 950), August 1985; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc950.txt (23 May 1998)

Mogul (Stanford); “Broadcasting Internet Datagrams” (RFC 919); October 1984; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc919.txt (23 May 1998)

Waitzmen, Partridge (BBN), Deering (Stanford); “Distance Vector Multicast Routing Protocol” (RFC 1075); November 1988; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1075.txt (23 May 1998)

Deering (Stanford); “Internet Group Multicast Protocol (IGMP)” (RFC 1112) August 1989; ftp://ftp.isi.edu/in-notes/rfc1112.txt (23 May 1998)

Braden (IETF); “Requirements for Internet Hosts – Communication Layers” (RFC 1122), October 1989; ftp://ftp.isi.edu/in-notes/rfc1122.txt (23 May 1998) (part of the IAB Standard 3, provides additional guidelines for the ARP)

Katz (Cisco); “Transmission of IP and ARP over FDDI Networks (RFC 1390/IAB Standard 36); January 1993; ftp://ftp.isi.edu/in-notes/rfc1390.txt (23 May 1998)

Fuller (BARRNet), Li (Cisco), Yu (MERIT), Varadhan (OARNet); “Classless InterDomain Routing (CIDR)” (RFC 1519), September 1993, http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1519.txt (23 May 1998)

Moy (Proteon); “Open Shortest Path First Version 2” (RFC 1583), March 1994; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1583.txt (23 May 1998)

Simpson (Daydreamer); “The Point-to-Point Protocol (PPP)” (RFC 1661/Standard 51); July 1994; ftp://ftp.isi.edu/in-notes/rfc1661.txt (23 May 1998)

Simpson (Daydreamer): “PPP in HDLC-like Framing” (RFC 1662/Standard 51); July 1994; ftp://ftp.isi.edu/in-notes/rfc1662.txt (23 May 1998)

Baker (Cisco); “Requirements for IP Version 4 Routers” (RFC 1812), June 1995; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1812.txt (23 May 1998)

Postel (IAB) “Internet Official Protocol Standards” (RFC 1880/IAB Standard 1); November 1995; ftp://ftp.isi.edu/in-notes/rfc1880.txt (23 May 1998)

Schulzrinne (GMD Fokus); “Real Time Transport Protocol (RTP) Profile for Audio and Video Conferences with Minimal Control” (RFC 1890); January 1996; http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1890.txt (23 May 1998)

ATM Protocols

ATM Forum specification, af-uni-0010.002 User-Network Interface (UNI) 3.1, 1994, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-sig-0061.000 User-Network Interface (UNI) Signaling v4.0, July 1996, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-sig-0076.000 User-Network Interface (UNI) Signaling Addendum, January 1997, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-pnni-0055.000 Private Network-to-Network Interface (PNNI) 1.0 (Phase 1), March 1996, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-pnni-0026.000 Interim Inter-switch Signaling Protocol (IISP) (PNNI Phase 0), December 1994, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-lane-0021 LAN Emulation (LANE) 1.0, January 1995, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

ATM Forum specification, af-mpoa-0087.000 Multiple Protocol Over ATM (MPOA) 1.0, July 1997, www.atmforum.com/atmforum/specs/approved.html (23 May 1998)

Obtaining IP Addresses:

For IP Addresses and support, the URL is http://www.netreg.navy.mil/. The e-mail address is shipreg@ncts.navy.mil, for ships and netreg@ncts.navy.mil for shore. Classified shore commands should use http://www.netreg.navy.smil.mil/ for the URL and netreg@ncts.navy.smil.mil for e-mail.

Obtaining NSAP Addresses:

Use the same address provided above in “Obtaining IP Addresses”. The DISA ATM Addressing plan is available on the World Wide Web at URL http://www.disa.atd.net/DISNATM_DOCS/.

5.6.2 Supporting Resources

Breyer and Riley, Switched and Fast Ethernet: How it Works and How to Use It, Ziff-Davis Press, Emeryvile, CA; 1995

Bryce, Using ISDN, Second Edition, Que Corporation, Indianapolis, IN, 1996

Hines, ATM, The Keys to high-Speed Broadband Networking, M&T Books, New York, NY; 1996